GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR

01197/11/RO
WP187

Avizul 15/2011 privind definiția consimțământului

Adoptat la 13 iulie 2011

Rezumat

Acest aviz prezintă o analiză detaliată a conceptului de consimțământ astfel cum este folosit în prezent în Directiva privind protecția datelor și în Directiva asupra confidențialității și comunicațiilor electronice. Bazându-se pe experiența membrilor grupului de lucru „articolul 29", avizul oferă numeroase exemple de consimțământ valabil și nevalabil, concentrându-se pe elementele cheie ale acestuia, cum ar fi înțelesul termenilor „manifestare", „liber exprimat", „specific", „neechivoc", „explicit", „informat" etc. Avizul clarifică , de asemenea, anumite aspecte legate de noțiunea de consimțământ. De exemplu, momentul în care trebuie obținut consimțământul, diferența dintre dreptul de opoziție și consimțământ etc.

Consimțământul este unul dintre temeiurile juridice pentru prelucrarea datelor cu caracter personal. Acesta are un rol important, însă nu exclude posibilitatea existenței, în funcție de circumstanțe, a altor temeiuri juridice care sunt poate mai adecvate, atât din perspectiva operatorului, cât și din perspectiva persoanei vizate. Dacă este utilizat în mod corect, consimțământul reprezintă un instrument care oferă persoanei vizate control asupra prelucrării datelor sale. Dacă este folosit în mod incorect, controlul persoanei vizate devine iluzoriu, iar consimțământul reprezintă un temei neadecvat pentru prelucrare.

Prezentul aviz este emis în parte ca răspuns la o solicitare din partea Comisiei, în contextul revizuirii Directivei privind protecția datelor, aflată în curs de desfășurare. Prin urmare, acesta conține recomandări care vor fi luate în considerare în procesul de revizuire. Aceste recomandări includ:

(i) clarificarea sensului sintagmei consimțământ „neechivoc" și explicarea faptului că numai consimțământul bazat pe declarații sau acțiuni care arată acordul constituie consimțământ valabil;

(ii) crearea de către operatorii de date a unor mecanisme care demonstrează obținerea consimțământului (în cadrul unei obligații generale de responsabilitate);

(iii) adăugarea unei cerințe explicite privind calitatea și accesibilitatea informațiilor care stau la baza consimțământului și

(iv) o serie de sugestii privind minorii și alte persoane aflate în incapacitate juridică.

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolul 29 și articolul 30 alineatul (1) litera (a) și alineatul (3),

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTUL AVIZ:

I. Introducere

Consimțământul persoanei vizate a constituit întotdeauna o noțiune cheie în domeniul protecției datelor cu caracter personal, însă nu este întotdeauna clar în ce situații este necesar consimțământul și care sunt condițiile care trebuie îndeplinite pentru ca acesta să fie valabil. Aceasta poate conduce la abordări diferite și la opinii divergente cu privire la bunele practici în statele membre, ceea ce poate reduce rolul persoanei vizate. Această problemă a crescut în importanță pe măsură ce prelucrarea datelor cu caracter personal a devenit un element din ce în ce mai evident în societatea modernă, atât în context online, cât și offline, adesea cu implicarea unor state membre diferite. Prin urmare, grupul de lucru „articolul 29" a hotărât să analizeze acest subiect în cadrul programului său de lucru pentru 2010-2011.

Consimțământul este , de asemenea, una dintre temele în legătură cu care Comisia a solicitat informații în contextul revizuirii Directivei 95/46/CE. Comunicarea Comisiei „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană"[1] stipulează: „*Comisia va avea în vedere modalități de clarificare și întărire a normelor privind consimțământul*." În comunicare, acest aspect este explicat[2] după cum urmează:

„Atunci când este necesar consimțământul în cunoștință de cauză, normele curente prevăd că, pentru prelucrarea datelor cu caracter personal, consimțământul persoanei respective ar trebui să fie o manifestare de voință, liberă, specifică și informată, prin care persoana își face cunoscut acordul privind prelucrarea datelor sale. Dar aceste condiții sunt în prezent interpretate în mod diferit în statele membre, variind de la obligația generală a existenței consimțământului în scris, până la acceptarea consimțământului implicit."

„Mai mult, în mediul electronic – din cauza opacității politicilor de confidențialitate – adeseori este mai dificil pentru persoane să își cunoască drepturile și să dea un consimțământ în cunoștință de cauză. Acest lucru este chiar și mai complicat de faptul că, în unele cazuri, nu este nici măcar clar ce ar însemna un consimțământ liber,

---

1 COM (2010) 609 final din 4.11.2010.

2 Primul raport al Comisiei referitor la punerea în aplicare a Directivei privind protecția datelor (95/46/CE) (COM(2003)265 final, menționa deja la pagina 17: „Conceptul de « consimțământ neechivoc » [articolul 7 litera (a)] în special, în comparație cu noțiunea de « consimțământ explicit » de la articolul 8 trebuie să fie clarificat și interpretat în mod uniform. Este necesar ca operatorii să știe ce este consimțământul valabil, în special în context online."

specific şi în cunoştinţă de cauză acordat pentru prelucrarea datelor, cum ar fi în cazul publicităţii comportamentale, în care setările browser-ului internet, se consideră de către unii, dar nu şi de către alţii, exprimă consimţământul utilizatorului."

„Prin urmare, ar trebui furnizate clarificări cu privire la condiţiile consimţământului persoanei vizate, pentru a se garanta întotdeauna un consimţământ în cunoştinţă de cauză şi a se asigura că persoana cunoaşte foarte bine faptul că îşi dă consimţământul şi pentru ce fel de prelucrare a datelor, conform articolului 8 din Carta drepturilor fundamentale a Uniunii Europene. Claritatea conceptelor-cheie poate favoriza, de asemenea, dezvoltarea unor iniţiative de autoreglementare în vederea găsirii unor soluţii practice conforme cu dreptul UE."

Pentru a răspunde cererii de informaţii a Comisiei şi pentru a-şi îndeplini programul de lucru pentru 2010-2011, grupul de lucru „articolul 29" s-a angajat să elaboreze un aviz. Scopul avizului este de a clarifica situaţia pentru a asigura o interpretare armonizată a cadrului juridic existent. În acelaşi timp, această acţiune se înscrie în logica avizelor precedente referitoare la alte dispoziţii cheie ale directivei[3]. Va trece o perioadă de timp până la modificarea potenţială a cadrului juridic existent, prin urmare clarificarea noţiunii actuale de „consimţământ" şi a principalelor sale elemente este cu siguranţă benefică. Clarificarea dispoziţiilor existente va arăta , de asemenea, care aspecte trebuie să fie îmbunătăţite. Astfel, pe baza acestei analize, avizul va încerca să formuleze recomandări de politică pentru a asista Comisia şi factorii de decizie în procesul de modificare a cadrului juridic aplicabil privind protecţia datelor.

Avizul are următoarea structură: după prezentarea unei imagini de ansamblu asupra evoluţiei în timp a cadrului legislativ şi asupra rolului consimţământului în legislaţia referitoare la protecţia datelor, se analizează diferitele elemente şi cerinţe necesare pentru un consimţământ valabil conform legilor aplicabile, inclusiv unele aspecte relevante ale Directivei 2002/58/CE asupra confidenţialităţii şi comunicaţiilor electronice. Analiza este ilustrată cu exemple practice bazate pe experienţa naţională. În ultima parte a avizului, pe baza acestei analize se fac recomandări potrivit cărora sunt necesare anumite dispoziţii pentru solicitarea şi obţinerea unui consimţământ valid în temeiul directivei. În acelaşi timp, avizul oferă spre analiză factorilor de decizie recomandări de politică în contextul revizuirii Directivei 95/46/CE.

II. Observaţii generale şi aspecte politice

II.1. Scurt istoric

În timp ce unele legi naţionale privind protecţia datelor/viaţa privată adoptate în anii '70 anticipau consimţământul ca fiind unul dintre temeiurile juridice pentru prelucrarea datelor cu caracter personal[4], acest subiect nu a fost abordat în Convenţia 108 a

[3] De exemplu, Avizul 8/2010 privind dreptul aplicabil, adoptat la 16.12.2010 (WP 179) şi Avizul 1/2010 privind conceptele de "operator" şi "persoană împuternicită de către operator", adoptat la 16.2.2010 (WP 169175).

[4] A se vedea, de exemplu, articolul 31 din Legea franceză nr. 78-17 din 6 ianuarie 1978 „relative a l'informatique, aux fichiers et aux libertés".

Consiliului Europei[5]. Nu există motive evidente pentru a nu acorda un rol mai important consimțământului în cadrul convenției[6].

La nivelul UE, utilizarea consimțământului drept criteriu pentru asigurarea legalității operațiunilor de prelucrare a datelor a fost prevăzută încă de la începutul procesului legislativ finalizat cu adoptarea Directivei 95/46/CE. Articolul 12 din propunerea Comisiei[7] din 1990 a stabilit caracteristicile consimțământului necesare pentru a asigura legalitatea operațiunilor de prelucrare de date: acesta trebuia să fie „*acordat în mod expres*" și „*specific*". Articolul 17, privind datele sensibile, stipula că acordarea consimțământului trebuia să se facă „*în mod expres și în scris*". Propunerea Comisiei modificată[8] din 1992 a introdus precizări în legătură cu definiția „consimțământului persoanei vizate" la articolul 2 alineatul (g) din textul actual, înlocuind articolul 12 anterior. Conform acesteia, consimțământul trebuia să fie „*liber exprimat și specific*". Sintagma „*acordat în mod expres*" a fost înlocuită cu acordarea consimțământului ca „*o manifestare expresă a voinței sale (a persoanei vizate)*". În memorandumul explicativ care însoțește propunerea modificată din 1992[9] se stipula că acordarea consimțământului se poate face verbal sau în scris. În ceea ce privește datele sensibile, rămânea valabil consimțământul „scris". În 1992, propunerea modificată a Comisiei a restructurat propunerea anterioară și a introdus articolul 7 care se referă la temeiurile juridice pentru prelucrare. Articolul 7 litera (a) prevede că prelucrarea poate avea loc dacă „*persoana vizată și-a dat consimțământul*"; lista inițială cuprindea, ca și în prezent, alte cinci temeiuri juridice (pe lângă consimțământ) care pot fi utilizate pentru a asigura legalitatea procesului de prelucrare a datelor.

Poziția comună a Consiliului[10] din 1995 a introdus definiția finală (actuală) a consimțământului: „*orice manifestare de voință liberă, specifică și informată prin care persoana vizată acceptă să fie prelucrate datele cu caracter personal care o privesc*". Principala modificare adusă poziției Comisiei din 1992 este reprezentată de eliminarea cuvântului „*expresă*" de lângă cuvântul „*manifestare*". În același timp, a fost introdus termenul „*neechivoc*" la articolul 7 alineatul (a), după cum urmează: „*dacă persoana vizată și-a dat consimțământul neechivoc*". Cerința privind acordarea consimțământul scris pentru datele sensibile a fost înlocuită cu necesitatea acordării „*consimțământului explicit*".

Motivele Consiliului[11] nu explicau în mod specific aceste modificări. Totuși, la pagina 4 se menționează: „*s-au adus ... o serie de modificări ... pentru a introduce un grad de flexibilitate care garantează o protecție egală ... dar nu duce la diminuarea nivelului de*

---

5 Convenția privind protecția persoanelor în ceea ce privește prelucrarea automată a datelor cu caracter personal (numită „Convenția 108"). Aceasta a intrat în vigoare la 1 octombrie 1985.

6 Convenția 108 a introdus noțiunile „prelucrare legală" și „scop legitim" (articolul 5) însă, spre deosebire de Directiva 95/46/CE, aceasta nu oferea o listă de criterii pentru prelucrarea legitimă a datelor. Consimțământul unei persoane vizate era luat în considerare numai în contextul asistenței reciproce (articolul 15). Totuși, necesitatea obținerii „consimțământului" a fost menționată ulterior în repetate rânduri în diferite recomandări ale Comitetului de miniștri.

7 Propunere de directivă privind protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, COM (90) 314 final, SYN 287 și 288, Bruxelles, 13 septembrie 1990.

8 Propunere modificată de directivă a Consiliului privind protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, COM (92) 422 FINAL- SYN 287, Bruxelles, 15 octombrie 1992.

9 A se vedea pagina 11 din Propunerea modificată de directivă a Consiliului privind protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, COM (92) 422 FINAL- SYN 287, Bruxelles, 15 octombrie 1992.

10 Poziția comună a Consiliului privind propunerea de directivă a Parlamentului și a Consiliului privind protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, (00/287) COD, adoptată la 15.3.1995.

11 A se vedea pagina 4 din poziția comună.

protecție; acestea permit aplicarea principiilor generale în mod eficient și nebirocratic, în conformitate cu diversitatea de modalități în care ... sunt prelucrate datele."

Rolul consimțământului a fost recunoscut în mod explicit în Carta drepturilor fundamentale a Uniunii Europene cu privire la protecția datelor cu caracter personal. Articolul 8 alineatul (2) stipulează că datele cu caracter personal pot fi prelucrate „*în temeiul consimțământului persoanei vizate sau într-un alt temei legitim stabilit prin lege*". Prin urmare, consimțământul este recunoscut ca aspect esențial al dreptului fundamental la protecția datelor cu caracter personal. În același timp, conform cartei, consimțământul nu este unicul temei juridic pentru prelucrarea datelor cu caracter personal; carta menționează explicit că se pot stabili, prin lege, alte temeiuri legitime, astfel cum este cazul Directivei 95/46/CE.

În concluzie, istoricul cadrului legislativ, în special în UE, arată rolul important al consimțământului în concepțiile privind protecția datelor și viața privată. În același timp, conform celor menționate, consimțământul nu a fost considerat unicul temei juridic pentru asigurarea legalității operațiunilor de prelucrare a datelor. Istoricul legislativ a Directivei 95/46/CE arată existența unui relativ consens privind condițiile consimțământului valid, mai precis: *liber exprimat, specific și informat*. Totuși, acesta arată , de asemenea, o anumită nesiguranță cu privire la modalitățile în care poate fi exprimat consimțământul – explicit, scris etc. Acest aspect este analizat în cele ce urmează.

II.2. Rolul conceptului: temei pentru asigurarea legalității

Temei general/specific:

Conceptul de consimțământ este utilizat în directivă atât ca temei general pentru asigurarea legalității (articolul 7), cât și ca temei specific în unele contexte specifice [articolul 8 alineatul (2) litera (a), articolul 26 alineatul (1) litera (a)]. Articolul 7 menționează consimțământul ca primul dintre cele șase temeiuri diferite pentru asigurarea legalității prelucrării datelor cu caracter personal, în timp ce articolul 8 prevede posibilitatea de a utiliza consimțământul pentru ca prelucrarea unor categorii speciale de date (sensibile), care, în caz contrar, ar fi interzisă, să fie legală. În acest ultim caz, standardul pentru obținerea consimțământului este mai înalt, întrucât acest tip de consimțământ depășește standardul general, deoarece trebuie să fie „explicit".

În plus, directiva permite interacțiunea cu alte legi, astfel cum se menționează în considerentul 23: „*Statele membre sunt împuternicite să asigure punerea în aplicare a protecției persoanei atât prin intermediul unui act general cu putere de lege privind protecția persoanelor în ceea ce privește datele cu caracter personal, cât și prin acte cu putere de lege în anumite sectoare*." Modul în care acest sistem funcționează în practică este complex: statele membre și-au pus în practică propriile abordări și, în unele cazuri, aceasta a condus la apariția unor diferențe.

Conceptul de consimțământ nu a fost întotdeauna transpus în mod literal la nivel național. De exemplu, consimțământul sub formă de concept general nu este definit în legislația franceză privind protecția datelor, însă sensul acestuia a fost explicat cu precizie și în mod consecvent în jurisprudența autorității de protecție a datelor (CNIL), în raport cu definiția din Directiva privind protecția datelor. În Regatul Unit, conceptul

de consimțământ a fost dezvoltat în cadrul dreptului comun cu referire la formularea din directivă. În plus, consimțământul a fost uneori definit în mod explicit în sectoare specifice, de exemplu în contextul confidențialității electronice, al e-guvernării sau al e-sănătății. Prin urmare, conceptul apărut în legislația specifică va interacționa cu cel creat în legislația generală privind protecția datelor.

Consimțământul este , de asemenea, o noțiune utilizată în alte ramuri ale dreptului, în special în dreptul contractelor. În acest context, pentru a garanta valabilitatea unui contract, se va ține seama de alte criterii decât cele menționate în directivă, cum ar fi vârsta, influența necuvenită etc. Nu există contradicții, ci suprapunere, între domeniile de aplicare a dreptului civil și a directivei: directiva nu se referă la condițiile generale de valabilitate a consimțământului într-un context de drept civil, însă nu le exclude. Aceasta înseamnă, de exemplu, că, pentru a evalua valabilitatea unui contract în contextul articolului 7 litera (b) din directivă, trebuie să se ia în considerare dispozițiile dreptului civil. Pe lângă aplicarea condițiilor generale pentru valabilitatea consimțământului conform dreptului civil, consimțământul necesar conform articolului 7 litera (a) trebuie să fie interpretat , de asemenea, ținând seama de articolul 2 litera (h) din directivă.

Interacțiunea cu alte legi nu este vizibilă numai la nivel național, ci și la nivel european. O interpretare similară a elementelor directivei a fost identificată în alte contexte, astfel cum arată o hotărâre judecătorească a Curții de Justiție în domeniul dreptului muncii[12]: obținerea consimțământului a fost necesară în contextul renunțării la un drept social. Instanța a interpretat conceptul de consimțământ în sensul Directivei 93/104 privind anumite aspecte ale organizării timpului de lucru. Aceasta menționa că „acordul lucrătorului" înseamnă acordarea consimțământului de către lucrător (nu de către un sindicat care reprezintă lucrătorul) și interpreta „acordul" (…) ca fiind consimțământul informat liber exprimat. În directivă se afirma , de asemenea, că lucrătorul care semnează un contract individual de muncă cu referire la un contract colectiv care permite prelungirea timpului de lucru nu îndeplinește condițiile conform cărora consimțământul trebuie să fie exprimat în mod liber și expres, cunoscând pe deplin toate faptele. Această interpretare a consimțământului într-un context specific este foarte apropiată de formularea din Directiva 95/46/CE.

Consimțământul nu este singurul temei pentru asigurarea legalității

Directiva prezintă clar consimțământul ca temei juridic. Totuși, unele state membre îl consideră un temei preferat, uneori apropiat de un principiu constituțional, legat de statutul protecției datelor ca drept fundamental. Alte state membre consideră consimțământul ca una dintre cele șase opțiuni, o cerință operațională cu nimic mai importantă decât celelalte opțiuni. Clarificarea relației dintre consimțământ și celelalte temeiuri juridice – de exemplu, în raport cu contractele, sarcinile de interes public sau de interes legitim al operatorului și dreptul de opoziție – va contribui la punerea în evidență a rolului consimțământului în situații specifice.

Ordinea în care sunt menționate temeiurile juridice la articolul 7 este relevantă, însă aceasta nu înseamnă că obținerea consimțământului este întotdeauna temeiul cel mai

[12] Hotărârea Curții (Marea Cameră) din 5 octombrie 2004, Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Döbele în cauzele comune C-397/01 – C-403/01.

adecvat pentru asigurarea legalității procesului de prelucrare a datelor cu caracter personal. La articolul 7 se menționează mai întâi consimțământul, apoi se enumeră celelalte temeiuri, inclusiv contractele și obligațiile legale, ajungând treptat la echilibrul intereselor. Trebuie să se remarce că pentru cele cinci motive enumerate după consimțământ trebuie să se efectueze un test al „necesității", care limitează strict contextele în care se aplică acestea. Acest lucru nu înseamnă că cerința privind obținerea consimțământului lasă mai multă marjă de manevră decât celelalte temeiuri indicate la articolul 7.

În plus, obținerea consimțământului nu elimină obligațiile operatorului stipulate la articolul 6 privind corectitudinea, necesitatea și proporționalitatea, precum și calitatea datelor. De exemplu, chiar dacă prelucrarea datelor cu caracter personal se bazează pe consimțământul utilizatorului, acest lucru nu justifică colectarea excesivă de date în raport cu un anumit scop.

De asemenea, obținerea consimțământului nu permite eludarea respectării altor dispoziții, precum cele ale articolului 8 alineatul (5). Numai în cazuri foarte rare consimțământul poate introduce în legalitate activități de prelucrare a datelor care ar fi altfel interzise, în special în ceea ce privește prelucrarea unor categorii de date sensibile (articolul 8) sau poate permite utilizarea datelor cu caracter personal în prelucrări ulterioare, indiferent dacă acest lucru corespunde sau nu scopului inițial. În principiu, consimțământul nu ar trebui privit ca o scutire de la respectarea celorlalte principii de protecție a datelor, ci ca o garanție. Consimțământul este în principal un temei juridic și nu împiedică aplicarea celorlalte principii.

Alegerea celui mai adecvat temei juridic nu este întotdeauna evidentă, în special între temeiurile de la articolul 7 literele (a) și (b). Conform articolului 7 litera (b), prelucrarea trebuie să fie necesară numai pentru executarea unui contract sau pentru luarea unor măsuri, la cererea persoanei vizate, înainte de încheierea contractului. Un operator de date care utilizează dispozițiile articolului 7 litera (b) ca temei juridic în contextul încheierii unui contract nu poate extinde aceste dispoziții pentru a justifica prelucrarea datelor într-o măsură mai mare decât cea necesară: acesta va trebui să introducă în legalitate prelucrarea suplimentară printr-un consimțământ specific, care trebuie să îndeplinească cerințele de la articolul 7 litera (a). Aceasta arată că este necesar un grad mai mare de precizie în termenii contractuali. În practică, aceasta înseamnă că obținerea consimțământului poate fi necesară ca o condiție suplimentară pentru o anumită parte a prelucrării. Prelucrarea trebuie să fie necesară pentru executarea unui contract; în caz contrar, trebuie să se obțină consimțământul (liber).

În unele tranzacții, este posibil să se aplice mai multe temeiuri juridice în același timp. Altfel spus, orice activitate de prelucrare a datelor trebuie să fie justificată permanent de unul sau mai multe temeiuri juridice. Aceasta nu exclude utilizarea simultană a mai multor temeiuri, cu condiția ca acestea să fie folosite în contextul potrivit. Colectarea anumitor date și prelucrarea suplimentară pot fi necesare în cadrul contractului cu subiectul datelor – articolul 7 alineatul (b); unele activități de prelucrare pot fi necesare în vederea îndeplinirii unei obligații legale – articolul 7 alineatul (c); colectarea de date suplimentare poate necesita obținerea unui consimțământ separat în acest sens – articolul 7 alineatul (a); alte activități de prelucrare pot fi legale în temeiul echilibrului intereselor – articolul 7 litera (f).

Exemplu: achiziționarea unui autovehicul
Operatorul de date este îndreptățit să prelucreze date cu caracter personal în diferite scopuri și în diferite temeiuri:
- datele necesare pentru achiziționarea autovehiculului: articolul 7 litera (b);
- pentru prelucrarea documentelor autovehiculului: articolul 7 alineatul (c);
- pentru serviciile de gestionare a clienților (de exemplu, pentru a asigura service-ul autovehiculului la diferite întreprinderi afiliate de pe teritoriul UE): articolul 7 alineatul (f);
- pentru a transfera datele către terți în vederea activităților de marketing ale acestora: articolul 7 alineatul (a).

II.3. Concepte asociate

Control

Conceptul de consimțământ este legat în mod tradițional de ideea potrivit căreia persoana vizată trebuie să dețină controlul asupra modului în care sunt utilizate datele sale. Din perspectiva drepturilor fundamentale, controlul exercitat prin consimțământ este un concept important. În același timp și din aceeași perspectivă, decizia unei persoane de a accepta o anumită operațiune de prelucrare a datelor ar trebui să facă obiectul unor cerințe riguroase, în special luând în considerare faptul că, prin decizia sa, persoana respectivă poate renunța la un drept fundamental.

Deși consimțământul are rolul său în acordarea controlului subiecților datelor, acesta nu reprezintă singurul mijloc de a realiza acest lucru. Directiva oferă și alte mijloace de control, în special dreptul de opoziție, însă acesta este un instrument diferit, utilizat într-o altă etapă a prelucrării, mai precis după începerea prelucrării și în baza unui temei juridic diferit.

Consimțământul este legat de conceptul de autonomie în materie de informații. Autonomia persoanei vizate este atât o condiție prealabilă, cât și o consecință a consimțământului: aceasta capătă astfel control asupra prelucrării datelor. Totuși, astfel cum se arată în capitolul următor, acest principiu are limite și există cazuri în care persoana vizată nu este în măsură să ia o decizie reală. Operatorul de date poate dori să utilizeze consimțământul exprimat de persoana vizată ca pe un mijloc de a-și transfera răspunderea către persoana respectivă. De exemplu, exprimându-și acordul pentru publicarea unor date cu caracter personal pe internet sau pentru transferarea lor unei societăți nesigure dintr-o țară terță, persoana vizată poate suferi prejudicii; operatorul de date poate susține că persoana vizată și-a dat acordul pentru acest lucru. De aceea, este important să reamintim că un consimțământ pe deplin valabil nu îl scutește pe operatorul de date de obligațiile sale și nu introduce în legalitate activități de prelucrare care ar fi incorecte în temeiul articolului 6 din directivă.

Conceptul de control este , de asemenea, legat de faptul că persoana vizată ar trebui să aibă posibilitatea de a-și retrage consimțământul. Retragerea nu este retroactivă, însă, în principiu, aceasta ar trebui să împiedice continuarea prelucrării datelor persoanei respective de către operator. Modul în care acest lucru funcționează în practică va fi analizat ulterior (capitolul III).

Transparența

Al doilea element al consimțământului se referă la informare: transparența față de persoana vizată. Aceasta este o condiție pentru deținerea controlului și pentru valabilitatea consimțământului. Transparența în sine nu este suficientă pentru ca prelucrarea datelor cu caracter personal să devină legală, însă reprezintă o condiție esențială pentru asigurarea valabilității consimțământului.

Pentru a fi valabil, consimțământul trebuie să fie informat. Aceasta înseamnă că, în momentul solicitării consimțământului, persoana vizată trebuie să fie în posesia tuturor informațiilor necesare și că aceste informații trebuie să vizeze aspectele de fond ale operațiunii de prelucrare căreia consimțământul trebuie să-i confere caracter legal. În mod normal, aceste informații ar trebui să fie cele enumerate la articolul 10 din directivă, însă aceasta depinde , de asemenea, de momentul și de circumstanțele în care este solicitat consimțământul.

Indiferent dacă s-a acordat sau nu consimțământul, transparența prelucrării datelor este , de asemenea, o condiție a corectitudinii, care are rolul său după momentul în care au fost furnizate informațiile inițiale.

Activitate/moment: modalități de a exprima consimțământul

Cel de-al treilea element se referă la modul în care este exercitat controlul: care sunt modalitățile în care poate fi exprimat consimțământul și când trebuie solicitat acesta pentru a garanta valabilitatea sa? Aceste întrebări au un impact decisiv asupra modului în care consimțământul este exercitat și interpretat.

Deși momentul în care trebuie solicitat consimțământul nu este precizat clar în directivă, acesta poate fi înțeles din formularea diferitelor dispoziții care arată că, de regulă, consimțământul trebuie să fie obținut înainte de începerea prelucrării[13]. Obținerea consimțământului înainte de începerea prelucrării datelor este o condiție esențială pentru ca prelucrarea să fie legală. Acest aspect este discutat mai pe larg în capitolul III.B referitor la Directiva asupra confidențialității și comunicațiilor electronice.

Consimțământul, privit ca autorizația acordată de persoana vizată de a prelucra datele care o privesc, poate fi exprimat în diferite moduri: articolul 2 litera (h) se referă la orice „manifestare"; acesta trebuie să fie neechivoc [articolul 7 litera (a)] și explicit pentru datele sensibile (conform articolului 8). Totuși, este esențial să se menționeze că exprimarea consimțământului este diferită de dreptul de opoziție, prevăzut la articolul 14. În timp ce, conform articolului 7 alineatul (a), operatorul nu poate prelucra datele până la obținerea consimțământului persoanei vizate, conform articolului 7 litera (f) operatorul poate prelucra datele, sub rezerva condițiilor și a garanțiilor, dacă persoana vizată nu și-a exercitat dreptul de opoziție. Astfel cum este menționat în documentul de lucru 114 al grupului de lucru, „*importanța consimțământului ca act pozitiv exclude de*

[13] De exemplu, versiunea germană a directivei (și Legea federală germană privind protecția datelor) utilizează termenul "Einwilligung". Acest termen este definit în Codul civil german ca „acord prealabil".

facto orice sistem în care persoana vizată ar avea dreptul de a se opune transferului numai după ce acesta a avut loc."[14].

Pentru aceste motive, dreptul de opoziție conform articolului 14 din directivă nu trebuie să fie confundat cu exprimarea consimțământului. Acesta din urmă reprezintă un temei juridic pentru prelucrarea datelor cu caracter personal în conformitate cu articolul 7 litera (a), articolul 8 alineatul (2) litera (a) și articolul 26 alineatul (1) sau astfel cum este stipulat în diferite dispoziții ale Directivei 2002/58/CE.

II.4. Utilizarea adecvată a consimțământului ca temei juridic

Este necesar să subliniem că obținerea consimțământului nu este întotdeauna mijlocul principal sau cel mai recomandabil de asigurare a legalității procesului de prelucrare a datelor cu caracter personal.

Consimțământul este uneori un temei neadecvat pentru justificarea prelucrării datelor cu caracter personal și își pierde valoarea atunci când este extins sau limitat pentru a fi adaptat unor situații în care nu a fost menit să fie utilizat. Utilizarea consimțământului „în contextul potrivit" este esențială. Dacă acesta este utilizat în situații care sunt neadecvate deoarece prezența elementelor care constituie consimțământul valabil este puțin probabilă, persoanele vizate devin foarte vulnerabile și, în practică, rolul acestora *se diminuează*.

Această abordare a fost deja susținută de grupul de lucru și de AEPD în contribuțiile lor la discuțiile pe marginea noului cadru legislativ privind protecția datelor. S-a afirmat în special că „*nu este întotdeauna clar în ce anume constă un consimțământ real și neechivoc. Unii operatori de date exploatează această incertitudine, utilizând metode neadecvate pentru acordarea unui consimțământ real și neechivoc*"[15], încălcând dispozițiile articolului 6 din directivă. În același sens, grupul de lucru articolul 29 menționează: „*complexitatea practicilor de colectare a datelor, modelele de afaceri, relațiile de vânzări și aplicațiile tehnologice depășesc de multe ori capacitatea sau dorința persoanei de a lua decizii în vederea controlării utilizării și transmiterii informațiilor printr-un act de voință*"[16].

Prin urmare, este important să se clarifice limitele consimțământului și să se asigure că numai consimțământul interpretat în conformitate cu dispozițiile legale este considerat valabil.[17]

---

[14] WP114 – Document de lucru al grupului de lucru „articolul 29" privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995.

[15] Avizul Autorității Europene pentru Protecția Datelor din 14 ianuarie 2011 privind Comunicarea Comisiei „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană".

[16] „Viitorul vieții private: contribuție comună la consultarea lansată de Comisia Europeană privind cadrul juridic pentru dreptul fundamental la protecția datelor cu caracter personal", 1 decembrie 2009, WP 168.

[17] Avizul Autorității Europene pentru Protecția Datelor din 14 ianuarie 2011, op.cit.

III. Analiza dispozițiilor

În cadrul acestei analize, ne vom concentra asupra Directivei 95/46/CE în capitolul III.A. Câteva fragmente relevante din Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice vor fi analizate în capitolul III.B. Trebuie precizat că aceste directive nu se exclud reciproc. Condițiile generale pentru valabilitatea consimțământului, astfel cum sunt prevăzute în Directiva 95/46/CE, se aplică atât în context online, cât și offline. Directiva 2002/58/CE specifică aceste condiții pentru anumite servicii online indicate explicit, tot în lumina condițiilor generale din Directiva privind protecția datelor.

III.A Directiva 95/46/CE

Conceptul de „consimțământ al persoanei vizate" este definit la articolul 2 litera (h) și este utilizat ulterior la articolele 7, 8 și 26. Rolul consimțământului este, de asemenea, menționat în considerentele 30 și 45. Aceste dispoziții și toate detaliile relevante vor fi discutate separat în cadrul prezentului capitol.

III.A.1. Articolul 2 litera (h)

Conform articolului 2 litera (h), „consimțământul persoanei vizate" înseamnă „*orice manifestare de voință, liberă, specifică și informată prin care persoana vizată acceptă să fie prelucrate datele cu caracter personal care o privesc*". Această definiție conține diferite elemente-cheie, care sunt discutate în cele ce urmează.

„... orice ... manifestare de voință ... prin care ... acceptă"

În principiu, nu există limite în ceea ce privește forma consimțământului. Totuși, pentru ca acesta să fie valabil, în conformitate cu directiva, trebuie să existe o manifestare. Chiar dacă este vorba despre „orice" formă de manifestare, trebuie să fie clar ce anume poate fi considerat o manifestare.

Forma manifestării (mai precis, modul în care este arătată voința) nu este definită în directivă. Din motive de flexibilitate, consimțământul „scris" a fost eliminat din textul final. Trebuie să se sublinieze că directiva menționează că este vorba de „orice" manifestare de voință, ceea ce oferă posibilitatea unei game largi de interpretări a conceptului de manifestare. Forma minimă de manifestare poate fi orice tip de semnal care este destul de clar pentru a putea arăta voința unei persoane vizate și pentru a fi înțeles de operatorul de date. Termenii „manifestare" și „prin care … acceptă" arată că este necesară, într-adevăr, o acțiune (spre deosebire de o situație în care consimțământul ar putea fi dedus din lipsa unei acțiuni).

Consimțământul ar trebui să includă orice manifestare de voință prin care persoana vizată *acceptă*: aceasta poate însemna o semnătură olografă la sfârșitul unui formular, dar și o declarație verbală care arată acordul sau un comportament din care poate fi dedus, în mod rezonabil, consimțământul. Pe lângă exemplul clasic al semnăturii, depunerea unei cărți de vizită într-un bol de sticlă ar putea , de asemenea, să se încadreze în definiție. Același lucru se aplică dacă o persoană își trimite numele și adresa unei organizații pentru a obține informații de la aceasta. În acest caz, ar trebui să

se înțeleagă că, prin acțiunea sa, persoana respectivă autorizează prelucrarea acestor date numai în măsura în care este necesară pentru prelucrarea și soluționarea cererii sale.

În avizul său privind utilizarea datelor de localizare în vederea furnizării de servicii cu valoare adăugată (WP115), grupul de lucru a analizat modul în care persoanele ar trebui puse în situația de a-și exprima consimțământul pentru servicii care necesită localizarea automată (de exemplu, posibilitatea de a apela un anumit număr pentru a obține informații privind condițiile meteorologice în locul în care te afli). În acest caz, a fost stabilit că apelarea numărului respectiv echivalează cu acordarea consimțământului pentru a fi localizat, cu condiția ca utilizatorii să fie informați în avans cu privire la prelucrarea datelor de localizare care îi privesc.

Exemplu: panouri publicitare Bluetooth
Există un mijloc de publicitate aflat în curs de dezvoltare care constă în panouri ce trimit mesaje prin care se solicită stabilirea unei conexiuni Bluetooth pentru a trimite anunțuri publicitare persoanelor care trec pe lângă panourile respective. Mesajele sunt trimise persoanelor care și-au activat dispozitivul Bluetooth la telefonul mobil. Activarea funcției Bluetooth nu reprezintă un consimțământ valabil (de exemplu, funcția Bluetooth ar putea fi activată în alte scopuri). Pe de altă parte, atunci când cineva a fost informat cu privire la acest serviciu și se apropie la distanță de câțiva centimetri de panou cu telefonul mobil, există, în mod normal, o manifestare de voință: aceasta arată ce persoane sunt într-adevăr interesate de primirea anunțurilor publicitare. Ar trebui să se considere că persoanele care și-au exprimat consimțământul și numai ele ar trebui să primească mesajele pe telefoanele lor mobile.

Este discutabil dacă absența unui comportament – sau, mai degrabă, comportamentul pasiv – poate fi interpretată , de asemenea, ca o manifestare de voință în situații foarte specifice (mai precis, într-un context complet neechivoc). Conceptul de „manifestare" este vast, însă pare să implice necesitatea unei acțiuni. Alte elemente din definiția consimțământului, precum și cerința suplimentară de la articolul 7 alineatul (a) conform căreia consimțământul trebuie să fie neechivoc, susțin această interpretare. Cerința ca persoana vizată să-și „arate" („*signify*") consimțământul pare să indice că inacțiunea este insuficientă și că este necesară o acțiune pentru a acorda consimțământul, deși există diferite tipuri de acțiuni, care trebuie analizate „în context".

În practică, în absența unui comportament activ din partea persoanei vizate, este dificil pentru operatorul de date să verifice dacă tăcerea a fost menită să exprime acordul sau consimțământul. De exemplu, este posibil ca un operator de date să nu aibă certitudinea necesară pentru a presupune că a fost exprimat consimțământul în următorul context: să ne imaginăm o situație în care operatorul de date trimite o scrisoare clienților prin care îi informează că are în vedere transferul datelor lor și că acest transfer nu va fi realizat dacă aceștia se opun în termen de două săptămâni; numai 10% din clienți răspund la această scrisoare. În acest exemplu, este contestabil că cei 90% care nu au răspuns sunt într-adevăr de acord cu transferul datelor. În astfel de cazuri, operatorul de date nu a obținut o indicație clară privind intenția persoanelor vizate. În plus, acesta nu are probe și nu poate, prin urmare, să dovedească faptul că a obținut consimțământul subiecților datelor. În practică, ambiguitatea unui răspuns pasiv face dificilă îndeplinirea condițiilor impuse de directivă.

"... liberă ..."

Consimțământul poate fi valabil numai dacă persoana vizată își poate exercita dreptul de a alege și nu există niciun risc de înșelăciune, intimidare, coerciție sau consecințe negative semnificative în cazul în care aceasta nu-și acordă consimțământul. În cazul în care consecințele exprimării consimțământului subminează libertatea de alegere a persoanei, consimțământul nu este liber. Chiar și în directivă se prevede, la articolul 8 alineatul (2) litera (a), că în unele cazuri, care trebuie stabilite de statele membre, interdicția de a prelucra unele categorii speciale de date cu caracter personal nu poate fi anulată de consimțământul persoanei vizate.

Un exemplu al situației de mai sus îl reprezintă cazul în care persoana vizată se află sub influența operatorului de date, fiind, de exemplu, angajatul acestuia. În această situație, deși nu neapărat întotdeauna, persoana vizată se poate afla într-o relație de dependență față de operatorul de date – din cauza naturii relației sau a unor circumstanțe speciale – și se poate teme că va fi tratat diferit dacă nu-și dă consimțământul pentru prelucrarea datelor.

Grupul de lucru a analizat limitele consimțământului în situații în care acesta nu poate fi acordat liber în mai multe dintre avizele sale, însă în special în cele privind dosarele electronice de sănătate (WP131), prelucrarea datelor în contextul ocupării forței de muncă (WP48), și prelucrarea datelor de către Agenția Mondială Anti-doping (WP162).

În WP131, grupul de lucru menționa: *„Consimțământul de «bună voie» presupune o decizie voluntară a unei persoane aflate în deplinătatea facultăților mentale, în lipsa unor constrângeri de orice fel, fie sociale, financiare, psihologice sau de altă natură. Orice consimțământ dat ca urmare a amenințării întreruperii tratamentului sau a tratamentului de calitate inferioară într-o circumstanță medicală nu poate fi considerat «de bună voie» ... În cazul în care un cadru medical trebuie să prelucreze date cu caracter personal în sistemul DES ca o urmare necesară și inevitabilă a actului medical, justificarea acestei prelucrări prin primirea acordului este falsă. Utilitatea acordului trebuie limitată la cazurile în care subiectul individual al datelor beneficiază de mai multe opțiuni reale și poate ulterior să-și retragă acordul fără a suferi neajunsuri."*[18]

În cazul în care, după retragerea consimțământului, prelucrarea datelor continuă sub alt temei juridic, pot apărea îndoieli cu privire la utilizarea anterioară a consimțământului ca temei juridic inițial: dacă prelucrarea ar fi putut fi efectuată încă de la început sub cel de-al doilea temei, punerea persoanei în situația de a-și acorda consimțământul pentru prelucrare poate fi considerată greșită sau injustă în mod inerent. Situația ar fi diferită dacă ar exista o modificare a circumstanțelor, de exemplu dacă ar apărea un nou temei juridic pe parcursul operațiunii de prelucrare, cum ar fi o nouă lege de reglementare a bazei de date vizate. Dacă noul temei se poate aplica prelucrării datelor conform dispozițiilor legale, prelucrarea poate continua. Totuși, în practică, aceste situații nu sunt frecvente. În principiu, consimțământul este considerat deficitar dacă nu este posibilă retragerea efectivă.

[18] WP162 privind Agenția Mondială Anti-doping ajunge la aceeași concluzie: „Sancțiunile și consecințele aferente unui posibil refuz al participanților de a se supune obligațiilor codului (de exemplu, cea privind completarea informațiilor privind localizarea) determină grupul de lucru să pună sub semnul îndoielii exprimarea liberă a consimțământului".

Grupul de lucru a adoptat o poziție consecventă privind interpretarea consimțământului liber în contextul ocupării forței de muncă[19]: „*în cazul în care este necesar consimțământul unui lucrător și acesta poate suferi prejudicii relevante potențiale sau reale în cazul neacordării consimțământului, consimțământul nu este valabil, deoarece nu respectă dispozițiile articolelor 7 și 8, mai precis nu este liber exprimat. Dacă lucrătorul nu are posibilitatea de a refuza, nu este vorba de consimțământ. ... O situație dificilă este cea în care acordarea consimțământului este o condiție a încadrării în muncă. În mod teoretic, lucrătorul poate să nu consimtă, însă cu consecința de a pierde o oportunitate de angajare. În astfel de situații, consimțământul nu este liber exprimat și, prin urmare, nu este valabil. Situația este chiar și mai clară în cazul în care toți angajatorii impun aceeași sau o condiție similară de angajare, așa cum se întâmplă adesea.*"

Exemplu: fotografii pe intranet
Consimțământul în contextul ocupării forței de muncă poate fi valabil, după cum arată următorul exemplu: o întreprindere decide să creeze un site intranet în care vor fi incluse numele și principalele atribuții ale angajaților. Fiecare angajat este întrebat dacă dorește ca fotografia sa să fie inclusă alături de nume. Persoanele care doresc ca fotografia lor să figureze pe intranet sunt invitate să trimită o fotografie la o adresă dată. După primirea informațiilor necesare, acțiunea persoanei de a trimite fotografia este considerată o manifestare a consimțământului. În cazul în care întreprinderea deține fotografii digitale ale tuturor angajaților și solicită consimțământul fiecăruia pentru a le încărca pe intranet în scopul menționat anterior, acțiunea angajaților de a face clic pe un buton pentru a-și da acordul este considerată , de asemenea, echivalentă cu acordarea unui consimțământul valabil. În ambele cazuri, alegerea angajaților de a-și include sau nu fotografia pe intranet este respectată pe deplin.

Contextul ocupării forței de muncă necesită o abordare specifică: în acest domeniu sunt importante aspectele culturale și sociale ale raportului de muncă, precum și modul în care principiile privind protecția datelor interacționează cu alte dispoziții legislative. În contextul ocupării forței de muncă, datele cu caracter personal pot fi prelucrate în diferite scopuri:

- Date necesare pentru îndeplinirea sarcinilor de către angajat: se aplică articolul 7 litera (b) – necesitatea pentru executarea unui contract
- Pentru a stabili dreptul angajaților de a achiziționa acțiuni: prelucrarea se poate face fie pe baza consimțământului – articolul 7 litera (a), fie poate fi considerată inerentă aspectelor administrative ale relației contractuale de muncă – articolul 7 litera (b)
- Prelucrarea numărului de securitate socială în scopuri legate de securitatea socială – articolul 7 litera (c) – îndeplinirea unei obligații legale, sau articolul 8 litera (b) – obligații în domeniul legislației privind ocuparea forței de muncă

[19] WP48 privind prelucrarea datelor cu caracter personal în contextul ocupării forței de muncă. WP114 – Document de lucru al grupului de lucru „articolul 29" privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995 – este , de asemenea, relevant în acest domeniu.

- Prelucrarea datelor etnice: în unele țări, aceasta poate fi , de asemenea, o obligație conform legislației privind ocuparea forței de muncă – articolul 8 litera (b), în timp ce în alte țări, aceasta este strict interzisă.

Deși există probabilitatea ca acordarea consimțământului să nu fie liberă în aceste situații, aceasta nu exclude complet utilizarea sa, cu condiția să existe suficiente garanții privind exprimarea cu adevărat liberă a consimțământului.

Deși relația ierarhică de subordonare este adesea principalul motiv care împiedică exprimarea liberă a consimțământului, există alte elemente contextuale care pot influența decizia persoanei vizate. Acestea pot fi, de exemplu, de natură financiară, emoțională sau practică. Colectarea datelor de către o autoritate publică poate influența , de asemenea, persoana vizată. Totuși, este dificil să se facă diferența între un simplu stimulent și un aspect care are o influență reală asupra libertății persoanei vizate de a-și exercita dreptul de a alege. Exemplele de mai jos urmăresc să ilustreze natura diferită a eforturilor sau a costurilor care afectează persoanele vizate și care ar putea să le influențeze decizia.

Exemplu: dosarele electronice de sănătate
În multe state membre, există tendința de a crea rezumate electronice ale fișelor medicale ale pacienților. Acest lucru permite furnizorilor de servicii medicale să acceseze informații-cheie oriunde pacientul are nevoie de tratament.
- În primul scenariu, crearea dosarului-rezumat este absolut voluntară, iar pacientul primește îngrijiri medicale indiferent dacă a consimțit sau nu la crearea acestuia. În acest caz, consimțământul pentru crearea dosarului este liber exprimat, deoarece pacientul nu suferă prejudicii dacă nu își acordă sau dacă își retrage consimțământul.
- În cel de-al doilea scenariu, există un stimulent financiar moderat pentru alegerea dosarelor electronice de sănătate. Pacienții care refuză crearea acestora nu suferă prejudicii în sensul că nu există modificări ale costurilor. Și în acest caz, se poate considera că pacienții sunt liberi să consimtă sau nu la aplicarea noului sistem.
- În cel de-al treilea scenariu, pacienții care refuză sistemul de dosare electronice de sănătate trebuie să suporte un cost suplimentar substanțial în comparație cu sistemul anterior de tarife, iar prelucrarea dosarului lor este întârziată în mod considerabil. Acesta reprezintă un prejudiciu clar pentru pacienții care nu-și acordă consimțământul, având scopul de a înregistra toți cetățenii în sistemul e-sănătate în termenul planificat. Prin urmare, în acest caz, consimțământul nu este liber într-o măsură suficientă. Astfel, ar trebui să se analizeze și existența altor motive legitime pentru prelucrarea datelor cu caracter personal sau aplicarea articolului 8 alineatul (3) din Directiva 95/46/CE.

Exemplu: scanerele corporale

Utilizarea scanerelor corporale devine din ce în ce mai frecventă în anumite spații publice, în special în aeroporturi, pentru accesul în zona de îmbarcare. Având în vedere că datele pasagerului sunt prelucrate în momentul efectuării scanării[20], prelucrarea trebuie să fie conformă cu unul dintre temeiurile juridice de la articolul 7. Trecerea prin scanerul corporal este prezentată uneori pasagerilor ca o opțiune, ceea ce implică faptul că prelucrarea datelor ar putea fi justificată prin consimțământul acestora. Totuși, refuzul de a trece prin scanerul corporal poate crea suspiciuni sau poate determina efectuarea de controale suplimentare, cum ar fi supunerea pasagerului la o percheziție corporală. Mulți pasageri acceptă să fie scanați deoarece astfel evită potențiale probleme sau întârzieri, prioritatea lor fiind de a se îmbarca în avion la timp. Acest consimțământ nu este exprimat în mod suficient de liber. Deoarece trebuie să se dovedească faptul că prelucrarea este necesară (pentru motive de securitate publică), temeiul juridic nu ar trebui să se regăsească la articolul 7 litera (a), ci într-o lege adoptată de organele legislative – articolul 7 litera (c) sau litera (e) – de unde să rezulte obligația pasagerilor de a coopera. Temeiul pentru utilizarea scanării corporale trebuie deci să fie legislația: legislația poate prevedea posibilitatea de a alege între scanare și percheziție, totuși această alegere ar fi oferită persoanelor numai dintr-o perspectivă complementară, ca parte a unor măsuri suplimentare.

Natura operatorului de date poate fi, de asemenea, decisivă cu privire la alegerea temeiului juridic pentru prelucrarea datelor cu caracter personal. Acest lucru se aplică în special operatorilor de date din sectorul public, unde prelucrarea datelor este legată în mod normal de îndeplinirea unei obligații legale, astfel cum se stipulează la articolul 7 litera (c) sau de aducerea la îndeplinire a unei sarcini de interes public, astfel cum se stipulează la articolul 7 litera (e). Prin urmare, utilizarea consimțământului persoanei vizate pentru asigurarea legalității procesului de prelucrare a datelor nu este temeiul juridic adecvat. Acest lucru este clar mai ales în cazul prelucrării datelor cu caracter personal de către autoritățile publice învestite cu puteri de exercitare a autorității – cum ar fi autoritățile de aplicare a legii care acționează în limita atribuțiilor lor, în domeniul poliției și al justiției. Autoritățile polițienești nu se pot baza pe consimțământul persoanei pentru măsuri care nu au fost prevăzute sau nu ar fi fost permise de legislație.

Trebuie să se recunoască totuși că, deși statul are datoria legală de a prelucra date cu caracter personal, persoana nu are întotdeauna obligația de a colabora. Pot exista situații în care subiecților datelor li se oferă „servicii cu valoare adăugată”, iar aceștia pot decide dacă să le utilizeze sau nu. Însă, în majoritatea cazurilor, prelucrarea este de fapt obligatorie. Adesea nu este ușor de stabilit dacă prelucrarea datelor cu caracter personal de către autoritățile publice se bazează în mod corect pe consimțământul persoanei. Prin urmare, prelucrarea datelor în sectorul public implică adesea sisteme hibride, care pot conduce la nesiguranță și abuzuri dacă prelucrarea este justificată în mod eronat prin consimțământ.

[20] A se vedea scrisoarea din 11 februarie 2009 din partea președintelui grupului de lucru „articolul 29” către dl. Daniel CALLEJA CRESPO, director al DG TREN privind scanerele corporale, ca răspuns la consultarea lansată de Comisie privind „impactul utilizării scanerelor corporale în domeniul securității aviatice asupra drepturilor omului, vieții private, demnității personale, sănătății și protecției datelor”. Disponibilă la adresa http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm.

Deși consimțământul poate reprezenta, în cazuri excepționale, un temei valabil pentru prelucrarea datelor cu caracter personal de către stat, trebuie să se verifice cu atenție fiecare caz în parte pentru a stabili dacă acordarea consimțământului s-a făcut în mod suficient de liber. Astfel cum arată următoarele exemple, atunci când operatorul de date este o autoritate publică, temeiul juridic pentru a aduce în legalitate prelucrarea datelor este îndeplinirea unei obligații legale, conform articolului 7 litera (c), sau îndeplinirea unei sarcini de interes public, conform articolului 7 litera (e), mai degrabă decât consimțământul.

Exemplu: e-guvernarea
În statele membre, se află în curs de dezvoltare noi carduri de identificare cu funcții electronice integrate într-un cip. Activarea serviciilor electronice ale cardului poate să nu fie obligatorie. Totuși, fără activare, s-ar putea ca utilizatorul să nu aibă acces la anumite servicii administrative, care ar putea fi dificil de accesat în alt mod (transferul unor servicii, acestea nemaifiind disponibile decât online, reducerea programului de lucru). Consimțământul nu poate fi invocat ca temei juridic pentru justificarea prelucrării. În acest caz, legea care reglementează dezvoltarea serviciilor electronice, cu toate măsurile de protecție adecvate, ar trebui să reprezinte temeiul relevant.

Exemplu: datele PNR (Passenger Name Record, registrul cu numele pasagerilor)
S-a pus în discuție dacă acordarea consimțământului de către pasageri poate fi utilizată pentru ca transferul datelor de rezervare („datele PNR") de către companiile aeriene europene către autoritățile Statelor Unite să fie legal. Grupul de lucru consideră că pasagerii nu își pot acorda în mod liber consimțământul, deoarece companiile aeriene sunt obligate să trimită datele înainte de zbor, prin urmare, dacă doresc să călătorească, pasagerii nu au, de fapt, de ales[21]. În acest caz, temeiul juridic nu este consimțământul pasagerului, ci, în conformitate cu articolul 7 litera (c), obligațiile stipulate în acordul internațional dintre UE și SUA privind prelucrarea și transferul datelor din registrul cu numele pasagerilor.

Exemplu: recensământul național
În cadrul unui recensământ național, populația trebuie să răspundă la diferite întrebări privind situația personală și profesională. La aceste întrebări trebuie să se răspundă în mod obligatoriu. În plus, chestionarul include și o întrebare cu privire la care se indică în mod clar că răspunsul este opțional, care se referă la mijlocul de transport utilizat. Deși, în mod evident, nu există posibilitatea consimțământului liber pentru partea principală a chestionarului, cetățenii pot alege liber dacă să răspundă sau nu la această ultimă întrebare opțională. Totuși, trebuie să se aibă în vedere că principalul scop urmărit de stat în alcătuirea acestor chestionare este de a obține răspunsuri. În termeni generali, consimțământul nu reprezintă un temei valabil în acest context.

"... specific ..."

Pentru a fi valabil, consimțământul trebuie să fie specific. Altfel spus, consimțământul superficial, fără a specifica scopul exact al prelucrării, nu este acceptabil.

[21] A se vedea Avizul 6/2002 al grupului de lucru „articolul 29" privind transmiterea către Statele Unite de către companiile aeriene a informațiilor generale referitoare la pasageri și a altor date.

Pentru a fi specific, consimțământul trebuie să fie inteligibil: acesta trebuie să se refere în mod clar și exact la domeniul de aplicare și la consecințele prelucrării datelor. Acesta nu poate să se aplice unei serii deschise de activități de prelucrare. Altfel spus, aceasta înseamnă că situațiile în care consimțământul poate fi utilizat sunt limitate.

Consimțământul trebuie să fie acordat în concordanță cu diferitele aspecte ale prelucrării, identificate clar. Trebuie să se știe care date sunt prelucrate și în ce scop. Această interpretare trebuie să se bazeze pe așteptările rezonabile ale părților. Prin urmare, „consimțământul specific" este legat intrinsec de faptul că acesta trebuie să fie informat. Consimțământul trebuie să fie precis cu privire la diferitele elemente pe care le presupune prelucrarea datelor: acesta nu poate fi susținut pentru a acoperi „toate scopurile legitime" ale operatorului de date. Consimțământul ar trebui să se refere la prelucrarea rezonabilă și necesară în raport cu scopul urmărit.

În principiu, ar trebui să fie suficient ca operatorii de date să obțină consimțământul o singură dată pentru diferite operațiuni în cazul în care acestea se încadrează în așteptările rezonabile ale persoanei vizate.

CEJ a pronunțat recent o hotărâre preliminară[22] cu privire la articolul 12 alineatul (2) din Directiva asupra confidențialității și comunicațiilor electronice, privind necesitatea reînnoirii consimțământului abonaților care și-au exprimat deja acordul pentru publicarea datelor lor cu caracter personal într-o listă de abonați în cazul în care aceste date sunt transferate spre publicare în alte liste de abonați. Curtea a hotărât că, în cazul în care abonatul a fost corect informat privind posibilitatea ca datele sale cu caracter personal să fie transferate unei întreprinderi terțe și acesta și-a exprimat consimțământul pentru publicarea datelor într-o astfel de listă de abonați, nu este necesară reînnoirea consimțământului abonatului pentru transferul datelor menționate, *cu condiția să se garanteze că datele respective nu vor fi utilizate în alte scopuri decât cele pentru care au fost colectate în vederea primei publicări a acestora (punctul 65)*.

În schimb, dacă operatorul de date are intenția de a prelucra datele în alte scopuri, este posibil ca acesta să trebuiască să obțină un consimțământ separat. De exemplu, consimțământul acordat poate acoperi informații atât despre noi produse, cât și despre anumite promoții, deoarece se consideră că aceste informații se încadrează în așteptările rezonabile ale persoanei vizate. Însă trebuie să se obțină un consimțământ separat și suplimentar pentru a transmite terților datele persoanei vizate. Nevoia de precizie în obținerea consimțământului ar trebui să fie analizată de la caz la caz, în funcție de scop (scopuri) sau de destinatorii datelor.

Trebuie să reamintim că prelucrarea poate avea diferite temeiuri juridice: unele date pot fi prelucrate deoarece sunt necesare pentru executarea unui contract încheiat cu persoana vizată, de exemplu pentru realizarea produsului și gestiunea serviciului, și poate fi necesar un consimțământ specific pentru prelucrarea datelor într-o măsură mai mare decât cea necesară în vederea executării contractului, de exemplu pentru a evalua capacitatea de plată (evaluarea bonității) a persoanei vizate.

---

[22] Hotărârea Curții din 5 mai 2011, Deutsche Telekom AG (Cauza C-543/09). Această cauză a început cu sesizarea Curții de către Instanța administrativă federală din Germania cu privire la listele de abonați telefonici și, în special, la interpretarea articolului 25 alineatul (2) din Directiva privind serviciul universal și a articolului 12 alineatul (2) din Directiva asupra confidențialității și a comunicațiilor electronice (2002/58/CE). Cauza este legată în mod evident de rolul special al listelor de abonați telefonici în Directiva privind serviciul universal.

Grupul de lucru a clarificat acest aspect cu privire la consimțământ în WP131 privind dosarele electronice de sănătate (DES): consimțământul „specific" trebuie să se refere la o situație bine definită, concretă, în care se urmărește prelucrarea datelor medicale. Prin urmare, „acordul general" al persoanei vizate – de exemplu, pentru colectarea datelor sale medicale în vederea creării unei fișe medicale electronice și pentru orice transfer ulterior al acestor date către cadre medicale implicate în tratament – nu reprezintă un consimțământ conform dispozițiilor articolului 2 litera (h) din directivă.

Același raționament este exprimat în WP115 privind utilizarea datelor de localizare în vederea furnizării de servicii cu valoare adăugată: „*definiția exclude în mod explicit consimțământul acordat în cadrul acceptării termenelor și condițiilor generale pentru serviciul de comunicații electronice oferit. ... În funcție de tipul de serviciu oferit, consimțământul se poate referi la o anumită operațiune sau poate reprezenta acordul pentru a fi localizat în mod permanent.*"

În hotărârea Curții menționată anterior în capitolul II, în cadrul secțiunii „Rolul consimțământului", chiar dacă nu se utilizează în mod explicit termenul „specific", raționamentul insistă, de asemenea, asupra faptului că acordarea consimțământului trebuie să fie specifică prin următoarea afirmație: „*nu este suficientă situația în care contractul de muncă al lucrătorului vizat face trimitere la un contract colectiv care permite o astfel de extindere*".

Exemplu: rețelele de socializare
Accesul la serviciile rețelelor de socializare este adesea condiționat de acceptarea a diverse tipuri de prelucrare a datelor cu caracter personal.

Utilizatorului i se poate cere să accepte primirea de publicitate comportamentală pentru a se înscrie într-o rețea de socializare, fără alte precizări sau opțiuni. Având în vedere importanța pe care au dobândit-o unele rețele de socializare, unele categorii de utilizatori (cum ar fi adolescenții) acceptă să primească publicitate comportamentală pentru a evita riscul de a fi excluși parțial din interacțiunile sociale. Utilizatorul ar trebui să fie pus în situația de a-și exprima consimțământul liber și specific pentru a primi publicitate comportamentală, independent de accesul său la serviciile rețelei de socializare. Se poate utiliza o fereastră de tip pop-up pentru a oferi utilizatorului această posibilitate.

Rețelele de socializare oferă posibilitatea de a utiliza aplicații externe. În practică, utilizatorul este adesea împiedicat să utilizeze o aplicație dacă nu acceptă să-și transmită datele dezvoltatorului aplicației într-o varietate de scopuri, inclusiv publicitatea comportamentală și revinderea către terți. Având în vedere că aplicația poate funcționa fără să fie necesară transmiterea datelor către dezvoltatorul aplicației, WP încurajează o mai mare precizie în obținerea consimțământului utilizatorului, mai precis obținerea unui consimțământ separat din partea utilizatorului pentru transmiterea datelor sale către dezvoltator în diferite scopuri. Se pot utiliza diferite mecanisme, cum ar fi ferestrele pop-up, pentru a oferi utilizatorului posibilitatea de a alege pentru care utilizare a datelor își exprimă acordul (transfer către dezvoltator; servicii cu valoare adăugată; publicitate comportamentală; transfer către terți etc.).

Specificitatea consimțământului înseamnă , de asemenea, că, în cazul în care scopul în care operatorul prelucrează datele se modifică la un moment dat, utilizatorul trebuie să fie informat în acest sens și pus în situația de a-și exprima consimțământul cu privire la noua prelucrare a datelor. Informațiile furnizate trebuie să vizeze în special consecințele refuzării modificările propuse.

"... informat ..."

Ultimul element din definiția consimțământului – însă nu și ultima cerință, astfel cum se va vedea în cele ce urmează – este caracterul său informat.

Articolele 10 și 11 din directivă stabilesc obligația de a furniza informații persoanelor vizate. Prin urmare, obligația de a furniza informații este distinctă, însă, în multe cazuri, aceasta este legată evident de consimțământ. Deși furnizarea de informații nu presupune întotdeauna acordarea consimțământului (se poate utiliza un alt temei de la articolul 7), consimțământul este întotdeauna condiționat de furnizarea prealabilă de informații.

În practică, aceasta înseamnă: *„consimțământul persoanei vizate (trebuie să fie) întemeiat pe judecarea și înțelegerea faptelor și implicațiilor unei decizii. Individul în cauză trebuie să primească, într-o manieră clară și inteligibilă, date exacte și complete despre toate aspectele relevante, în special despre cele menționate în articolele 10 și 11 ale directivei, precum natura datelor prelucrate, scopul prelucrării, destinatarii posibilelor transferuri și drepturile persoanei vizate. Aceasta include și cunoașterea consecințelor în cazul refuzului pentru prelucrarea în cauză."*[23]

În multe cazuri, consimțământul este solicitat în momentul colectării datelor cu caracter personal, atunci când începe procesul de prelucrare. În acest caz, informațiile care trebuie furnizate coincid cu cele enumerate la articolul 10 din directivă. Totuși, consimțământul poate fi , de asemenea, solicitat ulterior, atunci când se modifică scopul prelucrării. În acest caz, informațiile furnizate trebuie să vizeze aspectele necesare în contextul specific, în raport cu scopul.

Consimțământul informat este esențial în special în contextul transferului datelor cu caracter personal către țări terțe: „*este necesar ca persoana vizată (să fie) informată în mod corespunzător cu privire la riscurile specifice referitoare la transferul datelor sale către o țară în care nu există protecție adecvată*"[24].

Se pot identifica două tipuri de cerințe în vederea asigurării unei informări adecvate:

- Calitatea informațiilor – Modul în care sunt furnizate informațiile (sub forma unui text clar, fără utilizarea unui limbaj specializat, inteligibil, cu sens evident) este esențial atunci când se evaluează caracterul „informat" al consimțământului. Modul în care trebuie să fie oferite aceste informații depinde de context: acestea trebuie să poată fi înțelese de către un utilizator mediu.

[23] WP131 – Document de lucru privind prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate

[24] WP12 – Document de lucru: Transferurile de date cu caracter personal către țări terțe: aplicarea articolelor 25 și 26 din Directiva privind protecția datelor a UE. A se vedea , de asemenea, WP114 – Document de lucru al grupului de lucru „articolul 29" privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995.

- Accesibilitatea și vizibilitatea informațiilor – informațiile trebuie furnizate în mod direct persoanelor vizate. Nu este suficient ca informațiile să fie „disponibile" undeva. Curtea de Justiție a insistat asupra acestui aspect în hotărârea sa din 2004[25] privind un contract de muncă ce includea condiții care nu erau menționate explicit în contract, ci la care se făcea trimitere. Informațiile trebuie să fie vizibile clar (tipul și dimensiunea caracterelor), evidente și inteligibile. Se pot utiliza casete de dialog pentru a oferi informații specifice în momentul solicitării consimțământului. Astfel cum s-a precizat anterior cu privire la „consimțământul specific", instrumentele de informare online sunt în special utile în ceea ce privește serviciile rețelelor de socializare, cu scopul de a oferi suficientă precizie și claritate setărilor privind confidențialitatea. Anunțurile stratificate pot fi , de asemenea, un instrument util în acest caz, deoarece contribuie la furnizarea informațiilor adecvate într-un mod simplu și accesibil.

Odată cu trecerea timpului, se pot ivi îndoieli cu privire la menținerea valabilității unui consimțământ care era inițial întemeiat pe informații adecvate și suficiente. Din motive variate, oamenii își schimbă adesea părerile, deoarece alegerile lor inițiale au fost greșite sau din cauza modificării circumstanțelor, de exemplu copilul a crescut[26]. De aceea, ca o bună practică, operatorii de date ar trebui să facă eforturi pentru a reanaliza alegerile unei persoane după un anumit timp, informând-o, de exemplu, cu privire la opțiunea curentă și oferindu-i posibilitatea de a o confirma sau de a-și retrage consimțământul[27]. Perioada relevantă depinde desigur de context și de circumstanțele situației.

Exemplu: harta infracționalității
Poliția din unele state are în vedere publicarea unor hărți sau a unor informații de alt tip pentru a arăta unde au avut loc anumite tipuri de infracțiuni. De obicei, măsurile de protecție aferente procesului nu permit publicarea datelor cu caracter personal referitoare la victimele infracțiunilor, deoarece infracțiunile sunt raportate la zone geografice relativ extinse. Cu toate acestea, unele autorități din cadrul Poliției doresc să localizeze infracțiunile cu mai multă exactitate, în cazul în care victima infracțiunii acceptă acest lucru. În această situație, există posibilitatea să se creeze o legătură mai clară între subiectul datelor și locul în care a fost săvârșită infracțiunea. Totuși, victima nu este informată în mod specific că se vor publica pe internet informații identificabile care o privesc și modul în care pot fi folosite aceste informații. Prin urmare, consimțământul nu este valabil în acest caz deoarece este posibil ca victimele să nu înțeleagă exact măsura în care datele lor sunt făcute publice.

Cu cât prelucrarea datelor este mai complexă, cu atât cresc așteptările privind acțiunile operatorului de date. Cu cât este mai dificil pentru cetățeanul obișnuit să supravegheze și să înțeleagă toate elementele legate de prelucrarea datelor, cu atât mai multe eforturi trebuie să facă operatorul de date pentru a demonstra că a obținut consimțământul pe baza unor informații specifice și inteligibile.

Consimțământul, astfel cum este definit la articolul 2 litera (h), trebuie coroborat cu cerințele menționate ulterior în textul directivei. Articolul 7 adaugă la elementele

[25] A se vedea nota de subsol 12 (Capitolul II.2)
[26] Documentul de lucru 1/2008 privind protecția datelor cu caracter personal ale copiilor, WP 147, 18 februarie 2008.
[27] Grupul de lucru „articolul 29" a făcut recomandări similare în Avizul 171 privind publicitatea comportamentală online, adoptat la 22.6.2010.

definiției termenul „neechivoc”, iar articolul 8 introduce termenul „explicit” atunci când prelucrarea se referă la categorii specifice de date.

III.A.2. Articolul 7 litera (a)

În conformitate cu articolul 7 litera (a) din directivă, consimțământul neechivoc al persoanei vizate reprezintă un temei juridic pentru prelucrarea datelor cu caracter personal. Astfel, pentru a fi valabil, pe lângă îndeplinirea criteriilor stabilite la articolul 2 litera (h), consimțământul trebuie să fie *neechivoc*.

Consimțământul este considerat neechivoc atunci când procedura de solicitare și acordare a acestuia nu ridică *nicio îndoială* cu privire la intenția persoanei vizate de a-și acorda consimțământul. Altfel spus, manifestarea de voință prin care persoana vizată își arată acordul trebuie să fie lipsită de orice ambiguitate cu privire la intenția persoanei respective. Dacă există o îndoială rezonabilă cu privire la intenția persoanei, există ambiguitate.

Astfel cum se explică în continuare, această cerință obligă operatorii de date să creeze proceduri robuste pentru exprimarea consimțământului de către persoanele vizate, mai precis, fie să solicite consimțământul clar și specific, fie să utilizeze anumite tipuri de proceduri care arată consimțământul exprimat clar al persoanelor vizate. De asemenea, operatorul de date trebuie să aibă suficiente garanții că persoana care își exprimă consimțământul este chiar subiectul datelor. Această cerință este în special relevantă în cazul în care consimțământul se obține telefonic sau online.

Un aspect conex este legat de proba consimțământului. Operatorii de date care utilizează ca temei juridic consimțământul pot dori sau pot fi nevoiți să dovedească faptul că au obținut consimțământul, de exemplu, în contextul unui litigiu cu subiectul datelor. Într-adevăr, în unele cazuri, operatorilor li se poate solicita să facă proba consimțământului subiectului datelor în contextul acțiunilor de aplicare a legii. Prin urmare, ca o bună practică, operatorii de date ar trebui să instituie și să păstreze dovezi privind acordarea consimțământului, mai exact, consimțământul trebuie să fie verificabil.

Vom analiza în continuare următoarele metode de acordare a consimțământului și vom stabili dacă acestea determină exprimarea consimțământului neechivoc.

Declarațiile exprese care arată acordul, cum ar fi contractele semnate sau declarațiile scrise privind acordul sunt proceduri și mecanisme adecvate pentru acordarea consimțământului neechivoc. În același timp, în principiu, acestea oferă operatorului de date dovada obținerii consimțământului.

Exemplu: consimțământul pentru a primi informații promoționale prin poștă
Un hotel invită clienții să își scrie adresa poștală într-un formular dacă doresc să primească informații promoționale prin poștă. În cazul în care, după furnizarea informațiilor privind adresa, persoana semnează formularul, exprimându-și astfel acordul, consimțământul este neechivoc. În acest caz, consimțământul este atât expres, cât și în scris. Această procedură oferă operatorului de date dovezi adecvate privind obținerea consimțământului de la toți clienții în măsura în care acesta păstrează toate formularele semnate.

Totuși, nu toate formele de consimțământ care pot părea explicite sunt considerate valabile. Acest aspect a fost discutat în cadrul cauzei recente a CEJ (Volker und Markus Schecke/Land Hessen), care se referea la publicarea numelor beneficiarilor diferitor fonduri UE[28] și a sumelor primite de fiecare beneficiar. Avocatul General a analizat dacă au fost îndeplinite condițiile privind consimțământul neechivoc în situația în care persoanele au semnat o declarație conținând următorul text: „Recunosc că am luat la cunoștință faptul că articolul 44a din Regulamentul … nr. 1290/2005 impune publicarea informațiilor referitoare la beneficiarii [fondurilor] FEGA și FEADR și la sumele primite de fiecare beneficiar." Avocatul General a concluzionat: „*Avizarea prealabilă cu privire la faptul că va avea loc o anumită publicare nu este echivalentă cu consimțământul «neechivoc» pentru un mod specific de publicare a unor informații detaliate. Acest aviz nu poate fi corect descris nici ca «manifestarea liberă și specifică» a voinței solicitantului în temeiul definiției consimțământului persoanei vizate de la articolul 2 litera (h).*" Prin urmare, aceasta a stabilit că solicitanții nu și-au dat consimțământul pentru prelucrarea (mai precis, publicarea) datelor lor cu caracter personal în sensul articolului 7 litera (a) din Directiva 95/46/CE.[29]

Consimțământul expres poate fi acordat , de asemenea, online. Ca și în context offline, există metode adecvate de exprimare a consimțământului neechivoc, astfel cum arată următorul exemplu.

Exemplu: consimțământul online pentru a fi înscris într-un program de fidelitate
Site-ul internet al unui hotel include un formular de rezervare care le permite persoanelor să rezerve electronic camere. Formularul online în care persoanele introduc perioada dorită și informațiile referitoare la plată include, de asemenea, o căsuță vizibilă pe care persoanele pot să o bifeze dacă doresc ca datele lor să fie utilizate pentru a fi înscrise într-un program de fidelitate. Bifarea căsuței după primirea informațiilor relevante constituie un consimțământ specific, neechivoc, deoarece acțiunea de bifare a căsuței este suficient de clară și nu ridică îndoieli asupra dorinței persoanei de a fi înscrisă în programul de fidelitate.

Consimțământul expres poate fi acordat , de asemenea, verbal, prin declarații menite să arate acordul. Consimțământul expres verbal se acordă în următoarea situație.

Exemplu: consimțământul verbal pentru a primi informații promoționale
În timp ce clienții plătesc la părăsirea hotelului, recepționerul îi întreabă dacă doresc să își indice adresa pentru ca hotelul să le poată trimite informații promoționale. Persoanele care acceptă să își indice adresa, după ce au luat la cunoștință de cererea recepționerului și informațiile relevante, își acordă consimțământul în mod expres. Acțiunea de a-și indica adresa poate constitui o manifestare neechivocă a voinței persoanei. Totuși, operatorul de date poate alege să creeze mecanisme pentru a putea dovedi cu mai multă siguranță obținerea consimțământului.

[28] Fondul European de Garantare Agricolă (FEGA) și Fondul European Agricol pentru Dezvoltare Rurală (FEADR).

[29] Opinia Avocatului General Sharpston din 17 iunie 2010, Volker und Markus Schecke GbR, în cauzele comune C-92/09 și C-93/09. Trebuie să se remarce că CEJ a stabilit, în hotărârea pronunțată la 9 noiembrie 2010, că prelucrarea datelor nu a fost întemeiată pe consimțământ: „*63. Reglementarea în cauză a Uniunii Europene, care se limitează să prevadă că beneficiarii ajutoarelor vor fi informați în prealabil despre publicarea datelor care îi privesc, nu urmărește, așadar, să întemeieze prelucrarea datelor cu caracter personal pe care o impune pe consimțământul beneficiarilor vizați.*"

În unele situații, consimțământul neechivoc poate fi *dedus* din anumite acțiuni, în special atunci când acțiunile duc la concluzia evidentă că s-a obținut consimțământul. Totuși, aceasta presupune că informațiile relevante privind prelucrarea datelor au fost furnizate, oferind posibilitatea persoanei vizate de a lua o decizie (cine este operatorul de date, care este scopul prelucrării etc.).

Exemplu: consimțământul de a fi fotografiat
În timpul înregistrării la sosirea într-un hotel, recepționerul informează oaspeții că după-amiază va avea loc o ședință foto într-unul dintre restaurantele hotelului. Fotografiile selectate vor fi folosite pentru marketing, mai precis pentru broșuri tipărite de promovare a hotelului. Dacă oaspeții hotelului doresc să fie fotografiați, sunt invitați să fie prezenți în restaurant în perioada relevantă. Celor care nu doresc să fie fotografiați li se pune la dispoziție un alt restaurant.

Se consideră că oaspeții hotelului care – după ce au fost informați – hotărăsc să meargă la restaurant în perioada în care se desfășoară ședința foto și-au dat consimțământul pentru a fi fotografiați. Consimțământul acestora a fost dedus din acțiunea de a merge la restaurantul în care are loc ședința foto în perioada menționată. Prezența în restaurant reprezintă o manifestare a voinței persoanei vizate, care, în principiu, poate fi considerată neechivocă, deoarece există puține îndoieli cu privire la dorința persoanei care merge la restaurant de a fi fotografiată. Totuși, hotelul poate considera prudent să dețină documente justificative privind consimțământul obținut, în cazul în care valabilitatea acestui consimțământ este contestată în viitorul apropiat.

Astfel cum s-a menționat deja, cerințele privind consimțământul neechivoc se aplică atât online, cât și offline. Totuși, grupul de lucru remarcă faptul că este probabil ca riscul consimțământului echivoc să fie mai mare în context online; acest lucru necesită o atenție specială. Următorul exemplu arată un caz în care consimțământul dedus dintr-o anumită acțiune (participarea la un joc online) nu îndeplinește cerințele pentru a constitui consimțământ valabil.

Exemplu: joc online
Un furnizor de jocuri online le cere jucătorilor să își indice vârsta, numele și adresa pentru a participa la un joc online (distribuția jucătorilor se face în funcție de vârste și adrese). Site-ul internet prezintă un anunț care poate fi accesat printr-un link (deși accesarea acestui anunț nu este necesară pentru participarea la joc), care informează că, prin utilizarea site-ului respectiv (și, prin urmare, după furnizarea informațiilor), jucătorii consimt la prelucrarea datelor lor în scopul de a li se trimite informații de marketing de către furnizorul de jocuri online și de către terți.

Accesarea jocului și participarea la acesta nu sunt echivalente cu acordarea consimțământului neechivoc pentru prelucrarea ulterioară a datelor lor cu caracter personal în alt scop decât cel de a participa la joc. Participarea la joc nu implică intenția persoanei de a consimți la prelucrarea datelor într-o măsură mai mare decât cea necesară pentru a putea juca. Acest tip de comportament nu constituie o manifestare neechivocă a voinței persoanei de a i se utiliza datele în scopuri de marketing.

Exemplu: setările prestabilite privind confidențialitatea
Setările prestabilite ale unei rețele de socializare, pe care utilizatorii nu sunt nevoiți să le acceseze pentru a utiliza serviciile rețelei, permit întregii categorii „prieteni ai prietenilor" să facă toate informațiile cu caracter personal ale fiecărui utilizator accesibile pentru toți „prietenii prietenilor". Utilizatorii care nu doresc ca „prietenii prietenilor" să le vizualizeze informațiile trebuie să facă click pe un buton. Dacă rămân pasivi sau dacă nu efectuează acțiunea care constă dintr-un clic pe un buton, operatorul de date consideră că aceștia au consimțit ca datele lor să fie vizualizate. Totuși, este foarte discutabil dacă faptul de a *nu* face clic pe un buton înseamnă că persoana respectivă își dă consimțământul ca informațiile sale să fie accesate de toți prietenii prietenilor. Având în vedere că nu este clar dacă lipsa de acțiune este menită să însemne acordarea consimțământului, faptul de a nu face clic nu poate fi considerat consimțământ neechivoc.

Exemplul anterior ilustrează un caz în care persoana rămâne pasivă (mai precis, lipsa de acțiune sau „tăcerea"). Consimțământul neechivoc nu corespunde procedurilor de obținere a consimțământului pe baza inacțiunii sau a tăcerii persoanelor: tăcerea sau inacțiunea unei părți este echivocă în mod inerent (persoana vizată a dorit poate să încuviințeze sau poate că a dorit doar să nu întreprindă o acțiune). Următorul exemplu oferă încă o ilustrare a acestei situații.

Situația în care se consideră că persoanele vizate și-au dat consimțământul dacă nu au răspuns la o scrisoare prin care sunt informați că lipsa de răspuns este echivalentă cu consimțământul este echivocă. În situațiile de acest tip, comportamentul individual (sau, mai degrabă, absența acestuia) ridică mari îndoieli privind dorința persoanei respective de a-și arăta acordul. Faptul că persoana nu a întreprins nicio acțiune clară nu permite să se tragă concluzia că și-a dat consimțământul. Astfel, în această situație, nu sunt îndeplinite condițiile consimțământului neechivoc. În plus, astfel cum se ilustrează în continuare, va fi, de asemenea, foarte dificil pentru operatorul de date să ofere dovezi privind obținerea consimțământului de la persoana vizată.

Grupul de lucru a arătat caracterul inadecvat al consimțământului întemeiat pe tăcerea persoanelor vizate în contextul trimiterii de materiale de marketing direct prin e-mail. „*Consimțământul implicit de a primi aceste e-mailuri nu este compatibil cu definiția consimțământului din Directiva 95/46/CE. ... În mod similar, nici căsuțele deja bifate de pe site-uri, de exemplu, nu sunt în conformitate cu definiția din directivă.*"[30] Următorul exemplu confirmă această afirmație:

Exemplu: consimțământ nevalabil pentru utilizarea ulterioară a datelor clienților
Un distribuitor de cărți online trimite un e-mail clienților săi din programul de fidelitate, prin care îi informează că datele lor vor fi transferate unei companii de publicitate, care intenționează să le folosească în scopuri de marketing. Utilizatorii au la dispoziție un termen de două săptămâni pentru a răspunde la e-mail. Aceștia sunt informați că lipsa de răspuns este considerată consimțământ pentru transfer. Acest tip de mecanism, prin care consimțământul este dedus din lipsa de reacție a persoanelor

[30] Avizul 5/2004 privind comunicațiile nesolicitate în scopuri de marketing în temeiul articolului 13 din Directiva 2002/58/CE, adoptat la 27 februarie 2004 (WP90).

vizate, nu duce la obținerea unui consimțământ valabil și neechivoc. Nu este posibil să se stabilească în afara oricărei îndoieli că persoanele vizate au consimțit la transferul datelor numai pe baza lipsei răspunsului lor.

Din elementele prezentate anterior rezultă că, având în vedere cerința privind caracterul *neechivoc* al consimțământului, operatorii de date sunt încurajați *de facto* să instituie proceduri și mecanisme care nu lasă loc de îndoieli cu privire la acordarea consimțământului, fie pe baza unei acțiuni îndeplinite în mod expres de către persoana vizată, fie prin deducerea clară a acestuia dintr-o acțiune realizată de către persoana vizată.

Astfel cum s-a menționat anterior, ca o bună practică, operatorii de date ar trebui să aibă în vedere instituirea de măsuri și proceduri adecvate pentru a demonstra că s-a obținut consimțământul persoanelor vizate. Cu cât mediul în care lucrează operatorul este mai complex, cu atât mai multe măsuri sunt necesare pentru a garanta că obținerea consimțământului este verificabilă. Aceste informații trebuie puse la dispoziția autorității pentru protecția datelor la solicitarea acesteia.

III.A.3. Articolul 8 alineatul (2) litera (a)

Articolul 8 din directivă acordă o protecție specială unor „*categorii speciale de date*" care, prin natura lor, sunt considerate foarte sensibile. Prelucrarea acestor date este interzisă cu excepția cazului în care se aplică cel puțin una dintre excepțiile menționate. Articolul 8 alineatul (2) litera (a) prevede că interdicția nu se aplică dacă persoana vizată și-a dat *consimțământul explicit* pentru prelucrare.

În termeni legali, „consimțământul explicit" are același sens ca și consimțământul expres. Acesta se referă la toate situațiile în care persoanele vizate sunt puse în fața unei propuneri de a accepta sau a nu accepta o anumită utilizare sau divulgarea informațiilor lor cu caracter personal, iar aceștia răspund în mod activ la propunere, verbal sau în scris. De obicei, consimțământul explicit sau expres este exprimat în scris și însoțit de semnătura manuscrisă. De exemplu, consimțământul explicit este acordat atunci când persoanele vizate semnează un formular de consimțământ care arată clar de ce dorește operatorul de date să colecteze și să prelucreze ulterior datele cu caracter personal.

Deși consimțământul explicit se acordă în mod tradițional în scris, fie pe hârtie, fie în format electronic, astfel cum s-a arătat anterior, în capitolul III.A.2, acesta poate , de asemenea, să fie exprimat verbal. Acest lucru este dovedit de faptul că cerința de la articolul 8, conform căreia consimțământul trebuie să fie acordat în scris, a fost eliminată din versiunea finală a directivei. Totuși, astfel cum s-a arătat în capitolul menționat, consimțământul verbal poate fi dificil de dovedit, prin urmare, în practică, se recomandă operatorilor de date să solicite consimțământul scris din acest motiv.

Condiția referitoare la consimțământul explicit implică faptul că, în cazul în care consimțământul este dedus, acesta nu îndeplinește în mod normal cerințele de la articolul 8 alineatul (2). În acest sens, este bine să reamintim Avizul grupului de lucru „articolul 29" privind dosarele electronice de sănătate[31], care afirmă: *„În contrast cu dispozițiile articolului 7 din directivă, consimțământul în cazul datelor confidențiale cu*

[31] WP131 – Document de lucru privind prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate (DES).

*caracter personal și, în consecință, într-un DES, trebuie să fie **explicit**. Soluțiile care implică o renunțare nu întrunesc condițiile de a fi «explicite»”.*

Exemplu: date medicale pentru cercetare
Dacă un pacient este informat de către o unitate medicală că dosarul său medical va fi transmis unui cercetător cu excepția cazului în care pacientul se opune (prin apelarea unui număr de telefon), se consideră că nu sunt îndeplinite condițiile consimțământului informat.

Astfel cum s-a menționat anterior în capitolul II.A.2, persoanele își pot da consimțământul explicit, verbal și în scris, prin realizarea unei acțiuni afirmative pentru a-și exprima dorința de a accepta o anumită formă de prelucrare a datelor. În context online, consimțământul explicit poate fi acordat prin utilizarea semnăturilor electronice sau digitale. Acesta poate fi însă acordat , de asemenea, prin butoane pe care trebuie să se facă clic, în funcție de context, prin trimiterea de e-mailuri de confirmare, prin clic pe anumite icoane etc.[32]. Acceptarea procedurilor care necesită realizarea unei acțiuni afirmative de către persoana vizată este confirmată în mod explicit în considerentul 17 din Directiva asupra confidențialității și comunicațiilor electronice, care stipulează: „*Consimțământul poate fi acordat prin orice metodă potrivită acestui scop, care oferă indicații specifice și clare, acordate prin proprie voință, despre dorința utilizatorului, inclusiv prin bifarea unei căsuțe la vizitarea unui site Internet*”.

Consimțământul nu trebuie neapărat să poată fi consemnat pentru a fi valabil. Totuși, este în interesul operatorului de date să păstreze dovezi. Evident, greutatea dovezilor rezultate din diferite mecanisme poate varia, oferind mai multe sau mai puține probe privind consimțământul. Consimțământul obținut printr-un clic pe un buton și al cărui autor își arată identitatea numai printr-o adresă de e-mail are o valoare doveditoare mult mai mică decât un proces similar susținut, de exemplu, de mecanisme în care consimțământul este consemnat[33]. Necesitatea unor dovezi solide depinde , de asemenea, de tipul de date colectat și de scopul urmărit: semnătura electronică nu este necesară pentru a consimți la primirea de oferte comerciale, însă poate fi necesară pentru a consimți la prelucrarea anumitor tipuri de date financiare online. Consimțământul explicit acordat în context online trebuie să poată fi consemnat, astfel încât să poată fi accesat ulterior[34].

Având în vedere cele menționate anterior, se consideră că formularele de înregistrare online în care persoanele vizate trebuie să-și introducă datele de identificare și să-și dea consimțământul pentru prelucrarea datelor îndeplinesc condiția consimțământului explicit, cu condiția ca toate celelalte condiții să fie îndeplinite. De exemplu, pentru

[32] Această interpretare este conformă legislației UE, în principal în ceea ce privește comerțul electronic și utilizarea mai largă a semnăturilor digitale, care au determinat statele membre să-și modifice legislația care conținea cerințe formale ca documentele să fie „în scris” sau „manuscrise”, pentru ca echivalentele electronice ale acestora să fie acceptate de asemenea, cu îndeplinirea anumitor condiții.

[33] În acest sens, a se vedea, de exemplu, legislația din Grecia și Germania privind condițiile de acordare a consimțământului prin mijloace electronice, care cer consemnarea consimțământului într-un mod sigur, posibilitatea ca utilizatorul sau abonatul să-l poată accesa oricând și să-l poată retrage în orice moment [articolul 5 alineatul (3) din Legea elenă 3471/2006 privind protecția datelor cu caracter personal în sectorul comunicațiilor electronice; articolul 13 alineatul (2) din Legea federală germană privind teleserviciile, articolul 94 din Legea germană privind telecomunicațiile și articolul 28 alineatul (3) litera (a) din Legea federală germană privind protecția datelor).

[34] Prezentul aviz nu își propune să analizeze condițiile tehnice care trebuie îndeplinite de documentele electronice și semnăturile digitale pentru a li se acorda valoare egală cu cea a echivalentelor manuscrise ale acestora. Acest aspect nu se încadrează în domeniul de aplicare a legislației privind protecția datelor și a fost reglementat la nivelul UE.

crearea unui dosar de sănătate personalizate online, pacienții își pot acorda consimțământul prin indicarea datelor lor de contact și prin bifarea unei căsuțe specifice pentru a-și arăta acordul. Utilizarea unor metode de autentificare mai robuste – de exemplu, utilizarea semnăturilor electronice – conduce la același rezultat și constituie, în plus, o dovadă mai puternică[35].

În anumite cazuri, statele membre pot decide că o anumită operațiune de prelucrare a datelor trebuie introdusă în legalitate pe baza consimțământului și pot specifica un anumit tip de consimțământ. De exemplu, pentru a solicita eliberarea unui card de sănătate care oferă acces la istoricul medical, statele membre pot decide că persoanele care se înregistrează online trebuie să semneze cu un anumit tip de semnătură electronică. Această opțiune garantează că acordarea consimțământului s-a făcut în mod expres și oferă operatorului de date mai multă siguranță că va putea dovedi consimțământul persoanei respective.

III.A.4. Articolul 26 alineatul (1)

Articolul 26 alineatul (1) litera (a) menționează consimțământul ferm (neechivoc) al persoanei vizate ca derogare de la interdicția transferului de date către țările terțe cu nivel de protecție neadecvat. Afirmațiile anterioare cu privire la articolul 7 alineatul (a) se aplică și în acest caz. Aceasta înseamnă că, pe lângă cerințele referitoare la consimțământul valabil de la articolul 2 litera (g), consimțământul trebuie să fie , de asemenea, neechivoc.

Grupul de lucru „articolul 29" a dedicat mult timp formulării de orientări privind aplicarea articolelor 25 și 26 din directivă, inclusiv pentru derogarea referitoare la consimțământ. În acest context, este util să reamintim documentul WP12[36] al grupului de lucru privind sensul conceptului de consimțământ neechivoc: „*Având în vedere faptul că acordarea consimțământului trebuie să fie neechivocă, orice îndoială cu privire la acordarea consimțământului face derogarea inaplicabilă. Aceasta înseamnă probabil că multe situații în care consimțământul este implicit (de exemplu, deoarece o persoană a fost informată cu privire la transfer și nu s-a opus) nu se califică pentru aplicarea acestei derogări.*"

Având în vedere cele menționate anterior, consimțământul neechivoc este obținut mai degrabă atunci când persoanele realizează o acțiune afirmativă pentru a-și arăta acordul pentru transfer, de exemplu, prin semnarea unui formular de consimțământ sau realizarea altor acțiuni care arată în mod neîndoielnic că a fost acordat consimțământul.

În WP 114[37] privind utilizarea consimțământului pentru transferurile de date, grupul de lucru a afirmat: „*Este puțin probabil ca exprimarea consimțământului să ofere operatorilor de date un cadru legal adecvat pe termen lung în cazul transferurilor repetate sau chiar al transferurilor structurale în vederea prelucrării respective. De*

---

35 Aceasta deoarece anumite tipuri de semnături electronice (semnături electronice avansate bazate pe un certificat calificat și create de un dispozitiv special pentru crearea de semnături sigure) au în mod automat aceeași valoare juridică ca semnăturile manuscrise atunci când sunt considerate probe.

36 WP12 – Document de lucru: Transferuri de date cu caracter personal către țări terțe: aplicarea articolelor 25 și 26 din Directiva privind protecția datelor a UE, adoptată la 24 iulie 1998.

37 Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995, adoptat la 25.11.2005.

fapt, în special în cazul în care transferul face parte intrinsecă din prelucrarea principală (de exemplu, centralizarea unei baze de date mondiale a resurselor umane, care necesită aporturi continue și sistematice de date pentru a fi funcțională), operatorii de date se pot găsi în situații fără ieșire dacă numai unul din subiecții datelor hotărăște să-și retragă ulterior consimțământul. Mai precis, datele referitoare la o persoană care și-a retras consimțământul nu mai pot fi transferate; în lipsa acestuia, transferul ar continua să fie întemeiat parțial pe consimțământul persoanei vizate, însă trebuie să se găsească o soluție alternativă (contract, BCR etc.) pentru datele referitoare la persoanele care și-au retras consimțământul. Prin urmare, utilizarea consimțământului se poate dovedi a fi o „falsă soluție bună", simplă la prima vedere, însă complexă și dificilă în realitate."

III.A.5. <u>Consimțământul acordat de persoanele fără capacitate juridică deplină</u>

Conform Directivei 95/46/CE, nu există norme speciale privind obținerea consimțământului persoanelor fără capacitate juridică deplină, inclusiv copiii. Este important să se țină seama de această situație în contextul revizuirii Directivei privind protecția datelor. Pe lângă aspectele menționate anterior, consimțământul acestor persoane prezintă probleme proprii, specifice.

În ceea ce privește copiii, condițiile pentru acordarea consimțământului valabil variază de la un stat membru la altul. Grupul de lucru „articolul 29" a abordat în mai multe rânduri problema consimțământului copiilor și a analizat practicile naționale[38].

Publicațiile precedente arată că, atunci când este necesar consimțământul copilului, legislația poate să dispună obținerea consimțământului copilului și al reprezentantului acestuia sau numai a consimțământului copilului dacă acesta este deja matur. Vârsta la care se aplică prima sau a doua regulă variază. Nu există proceduri armonizate pentru verificarea vârstei unui copil.

Lipsa normelor generale în domeniu conduce la o abordare fragmentată și nu recunoaște necesitatea unei protecții specifice pentru copii în anumite circumstanțe, din cauza vulnerabilității acestora și deoarece această situație creează insecuritate juridică, în special în ceea ce privește modul în care trebuie să se obțină consimțământul copiilor.

Grupul de lucru consideră că lipsa armonizării în domeniu are consecințe asupra securității juridice. Armonizarea condițiilor care permit persoanelor aflate în incapacitate juridică să-și exercite drepturile la nivelul UE, în special în ceea ce privește pragul de vârstă, ar aduce cu siguranță garanții suplimentare. Totuși, grupul de lucru înțelege că acest aspect iese din domeniul de aplicare a protecției datelor, deoarece are legătură mai degrabă cu aspectele de drept civil. Grupul de lucru atrage atenția Comisiei asupra provocărilor existente în domeniu.

În plus, grupul de lucru „articolul 29" consideră că interesele copiilor și ale altor persoane lipsite de capacitate juridică deplină ar fi mai bine protejate dacă directiva ar conține dispoziții suplimentare, vizând în mod specific colectarea și prelucrarea

[38] WP147 – Documentul de lucru 1/2008 privind protecția datelor cu caracter personal ale copiilor (Orientări generale și cazul special al școlilor); WP160 Avizul 2/2009 privind protecția datelor cu caracter personal ale copiilor (Orientări generale și cazul special al școlilor).

ulterioară a datelor acestora. Astfel de dispoziții ar putea preciza circumstanțele în care este necesar consimțământul reprezentantului, pe lângă sau în locul consimțământului persoanei aflate în incapacitate și ar putea stabili situații în care consimțământul nu poate fi folosit ca temei pentru legalizarea prelucrării datelor cu caracter personal. Ar trebui , de asemenea, să se introducă cerința de a utiliza mecanisme de verificare a vârstei online. Există mecanisme diferite și praguri diferite. De exemplu, verificarea vârstei ar putea să se bazeze nu pe o singură regulă, ci pe un sistem flexibil, în care mecanismele utilizate să depindă de circumstanțe, precum tipul de prelucrare (scopurile), gradul de risc, tipul de date colectate, modul de utilizare a datelor (dacă datele sunt menite sau nu să fie divulgate) etc.

III.B. Directiva 2002/58/CE

Directiva asupra confidențialității și comunicațiilor electronice (Directiva 2002/58/CE), recent modificată[39], este *lex specialis* pentru Directiva 95/46/CE deoarece prezintă sistemul specific unui sector în ceea ce privește confidențialitatea și comunicațiile electronice. Majoritatea dispozițiilor sale se aplică numai furnizorilor de servicii publice de comunicații electronice (de exemplu, furnizorii de servicii de telefonie, de internet etc.).

Unele dintre dispozițiile Directivei asupra confidențialității și comunicațiilor electronice desemnează consimțământul ca un temei juridic pe care furnizorii de servicii publice de comunicații electronice îl pot utiliza pentru a prelucra date[40]. Această situație se aplică, de exemplu, utilizării datelor de localizare sau de transfer.

Grupul de lucru „articolul 29" consideră util să analizeze anumite aspecte de interes deosebit privind utilizarea consimțământului din Directiva asupra confidențialității și comunicațiilor electronice. În acest scop, vom aborda următoarele cinci aspecte:

a) Relația dintre definiția și sensul general al consimțământului în Directiva 95/46/CE și în Directiva asupra confidențialității și comunicațiilor electronice, pe baza articolului 2 alineatul (2) litera (f) din aceasta din urmă.

b) Dacă, pentru a încălca regula confidențialității comunicațiilor (de exemplu, pentru a monitoriza sau a intercepta o comunicație telefonică), este necesar să se obțină consimțământul uneia sau al ambelor părți ale comunicației. Acest aspect este reglementat de articolul 6 alineatul (3) și de articolul 5 alineatul (1).

c) Momentul în care trebuie să se obțină consimțământul. Acest aspect este abordat în diferite dispoziții ale Directivei asupra confidențialității și comunicațiilor electronice, inclusiv în articolul 5 alineatul (3), articolul 6 și articolul 13.

---

[39] Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile electronice de comunicații, Directiva 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și Regulamentul (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului, 18.12.2009.

[40] Datele de transfer înseamnă datele prelucrate în scopul transmiterii unei comunicații într-o rețea de comunicații electronice sau pentru facturarea respectivei comunicații electronice, inclusiv datele legate de ruta, durata sau momentul în care a avut loc o comunicație.

d) Domeniul de aplicare a dreptului de opoziție și modul în care acesta este diferit de consimțământ. Această diferență poate fi analizată în temeiul articolul 13 din Directiva asupra confidențialității și comunicațiilor electronice.

e) Posibilitatea de retragere a consimțământului, astfel cum se prevede în mod explicit la articolul 6 alineatul (3) și la articolul 9 alineatele (3) și (4) din Directiva asupra confidențialității și comunicațiilor electronice.

III.B.1. Articolul 2 litera (f) - Consimțământul și relația sa cu Directiva 95/46/CE

„*consimțământul utilizatorului sau al abonatului*"

Articolul 2 din Directiva asupra confidențialității și comunicațiilor electronice menționează explicit că, în sensul Directivei 2002/58/CE, se aplică definițiile din Directiva 95/46/CE. La articolul 2 litera (f) se stipulează: „*acordul unui abonat sau utilizator înseamnă consimțământul acordat de subiectul datelor din Directiva 95/46/CE*".

Aceasta înseamnă că, atunci când este necesară obținerea consimțământului în temeiul Directivei asupra confidențialității și comunicațiilor electronice, criteriile pentru stabilirea valabilității consimțământului sunt aceleași cu cele prevăzute de Directiva 95/46/CE, mai precis definiția de la articolul 2 litera (g) și dispoziția specifică de la articolul 7 litera (a). Faptul că, în Directiva asupra confidențialității și comunicațiilor electronice, consimțământul trebuie interpretat prin trimitere la articolul 2 litera (g) coroborat cu articolul 7 litera (a) este confirmat în considerentul 17[41].

III.B.2. Articolul 5 alineatul (1) – Consimțământul este necesar de la una sau de la ambele părți

„ … *acordul utilizatorului în cauză*…"

Articolul 5 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice protejează confidențialitatea comunicațiilor prin interzicerea oricărei forme de interceptare sau supraveghere a comunicațiilor fără consimțământului tuturor utilizatorilor în cauză.

În acest caz, la articolul 5 alineatul (1) se solicită consimțământul „*tuturor utilizatorilor în cauză*", altfel spus, al celor două părți ale unei comunicări. Consimțământul uneia dintre părți nu este suficient.

În contextul elaborării Avizului său 2/2006[42], grupul de lucru „articolul 29" a analizat mai multe servicii care presupun examinarea conținutului e-mailurilor și, în unele cazuri, urmărirea deschiderii e-mailurilor. Grupul de lucru și-a exprimat preocuparea că, în cadrul acestor servicii, una dintre părțile participante la comunicare nu a fost

[41] Acesta prevede următoarele: „*În sensul prezentei directive, consimțământul ... trebuie să aibă aceeași însemnătate ca și consimțământul acordat de subiectul datelor așa cum este definit și specificat de Directiva 95/46/CE".*

[42] Avizul 2/2006 privind aspecte referitoare la viața privată legate de furnizarea de servicii de examinare a e-mailurilor, adoptat la 21.2.2006 (WP118).

informată. Pentru ca aceste servicii să fie în conformitate cu articolul 5 alineatul (1), este necesar consimțământul ambelor părți ale comunicării.

III.B.3 Articolul 6 alineatul (3), articolele 9, 13 și articolul 5 alineatul (3) – Momentul în care trebuie obținut consimțământul

„ *... să fi primit informații clare și complete ...”*

Diferite dispoziții ale Directivei asupra confidențialității și comunicațiilor electronice conțin exprimări explicite sau implicite care arată că acordarea consimțământului trebuie să aibă loc înainte de prelucrare. Aceasta corespunde, de asemenea, dispozițiilor Directivei 95/46/CE.

Articolul 6 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice include o mențiune explicită privind consimțământul prealabil al abonatului sau utilizatorului vizat, impunând obligația de a oferi informații și de a obține consimțământul prealabil înainte de prelucrarea datelor de transfer în scopul serviciilor de comunicații electronice de marketing sau al serviciilor cu valoare adăugată. Pentru anumite tipuri de servicii, consimțământul poate fi obținut de la abonat în momentul înscrierii pentru primirea serviciului respectiv. În alte cazuri, este posibil ca acesta să fie obținut direct de la utilizator. O abordare similară apare la articolul 9 privind prelucrarea datelor de localizare, altele decât datele de transfer. Furnizorul de servicii trebuie să informeze utilizatorii sau abonații – *înainte de a obține consimțământul lor* – cu privire la tipul de date de localizare, altele decât datele de transfer, care *vor fi* prelucrate. Articolul 13 introduce cerința de a obține consimțământul prealabil al abonaților pentru a utiliza sistemele de apelare automată fără intervenție umană, faxul sau e-mailul în scopuri de marketing direct.

Articolul 5 alineatul (3) conține o regulă specifică cu privire la stocarea sau accesarea informațiilor din echipamentul terminal al unui abonat, inclusiv în scopul urmăririi activităților online ale abonatului. Deși la articolul 5 alineatul (3) nu se folosește cuvântul „prealabil”, acest lucru se poate deduce clar din formularea dispoziției.

Este logic ca obținerea consimțământului să aibă loc *înainte* de începerea procesului de prelucrare a datelor. În caz contrar, prelucrarea efectuată între momentul în care aceasta a început și momentul în care a fost obținut consimțământul ar fi ilegală deoarece nu există temei juridic. În plus, în astfel de cazuri, dacă persoana vizată ar hotărî că nu dorește să-și dea consimțământul, prelucrarea datelor care a avut deja loc ar fi ilegală din aceleași motive.

Așadar, rezultă că atunci când este *necesară* obținerea consimțământului, aceasta trebuie să aibă loc înainte de începerea prelucrării datelor. Posibilitatea de a începe prelucrarea fără a fi obținut consimțământul persoanelor vizate este legală numai în cazul în care Directiva privind protecția datelor sau Directiva asupra confidențialității și comunicațiilor electronice prevăd, în loc de obținerea consimțământului, un temei juridic alternativ pentru prelucrare și fac trimitere la dreptul de a se opune sau de a refuza prelucrarea datelor. Aceste mecanisme se disting clar de consimțământ. În aceste cazuri, este posibil ca prelucrarea să fi început deja și persoana vizată are dreptul de a se opune sau de a o refuza.

O ilustrare a acestei situații poate fi identificată la articolul 5 alineatul (3) din Directiva anterioară asupra confidențialității și comunicațiilor electronice, care prevedea (sublinierea noastră): „*folosirea rețelelor de comunicații electronice pentru a stoca sau a accesa informații stocate în echipamentul terminal al unui abonat sau utilizator este permisă doar cu condiția ca abonatul sau utilizatorul în cauză să fi primit informații clare și complete, în conformitate cu Directiva 95/46/CE, inter alia, cu privire la scopul prelucrării de către operatorul de date, care îi oferă dreptul de a refuza această prelucrare.”*. Acest text trebuie să fie comparat cu noua formulare a articolului 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice astfel cum a fost modificată de Directiva 2009/136/CE[43], care stipulează că „ *(...) stocarea sau accesarea informațiilor stocate în echipamentul terminal al unui abonat sau utilizator este permisă doar cu condiția ca abonatul sau utilizatorul în cauză să-și fi dat consimțământul în acest sens (...).”* Consecințele acestei modificări a formulării articolului 5 alineatul (3) au fost explicate de grupul de lucru „articolul 29” în avizul său 2/2010 privind publicitatea comportamentală online[44]. Diferența dintre refuz și consimțământ este dezvoltată , de asemenea, în capitolul următor.

În multe cazuri în care Directiva asupra confidențialității și comunicațiilor electronice sau Directiva privind protecția datelor prevăd posibilitatea de a refuza prelucrarea datelor cu caracter personal, temeiul juridic al prelucrării inițiale a datelor este *altul* decât consimțământul, de exemplu un contract aflat în vigoare. Acest aspect este mai bine ilustrat în secțiunea următoare, care analizează articolul 13 din Directiva asupra confidențialității și comunicațiilor electronice.

III.B.4. Articolul 13 alineatele (2) și (3) – dreptul de opoziție și diferențierea acestuia de consimțământ

„ ... clientului să i se ofere în mod clar și distinct posibilitatea de a se opune ...”

Articolul 13 din Directiva asupra confidențialității și comunicațiilor electronice prevede utilizarea consimțământului pentru a trimite comunicații electronice în scopuri de marketing direct în mod legal. Această prevedere are la bază un principiu standard și o dispoziție specifică.

În ceea ce privește utilizarea sistemelor de apelare automată, a faxului și a e-mailului, este necesar consimțământul prealabil al persoanei vizate.

Dacă destinatarul unei comunicații comerciale este un client actual și comunicația are scopul de a promova produsele sau serviciile proprii ale furnizorului sau produse și servicii similare, nu este necesar să se acorde consimțământul, ci să se garanteze că

[43] Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor electronice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului. Text cu relevanță pentru SEE, *J.O. L 337, 18.12.2009, P. 0011 - 0036*

[44] Avizul din 22 iunie 2010, WP 171: aspectul privind existența sau nu a posibilității exprimării consimțământului prin „setările adecvate ale browser-ului sau ale unei alte aplicații” [considerentul 66 din Directiva 2009/136/CE] este abordat în mod explicit la punctul 4.1.1 din WP 171.

persoanei „*i se oferă posibilitatea de a se opune*", conform articolului 13 alineatul (2). În considerentul 41 se explică de ce autoritățile legislative, în acest caz, nu au solicitat exprimarea consimțământului: „*În contextul unei relații client existente, este firesc să se permită folosirea detaliilor de contact electronice pentru ofertele de produse sau servicii similare*." Așadar, în principiu, relația contractuală dintre persoană și furnizorul de servicii este temeiul juridic care permite primul contact prin e-mail. Totuși, persoanele ar trebui să aibă posibilitatea de a se opune contactelor ulterioare. Astfel cum a arătat deja grupul de lucru: „*Această posibilitate trebuie să continue să fie oferită la fiecare mesaj ulterior de marketing direct, în mod gratuit, cu excepția eventualelor costuri pentru transmiterea acestui refuz*".[45]

Necesitatea consimțământului trebuie să fie diferențiată de dreptul de opoziție. Astfel cum se arată mai sus în capitolul III.A.2, consimțământul întemeiat pe lipsa de acțiune a persoanelor, de exemplu, căsuțele deja bifate, nu îndeplinesc condițiile consimțământului valabil, conform Directivei 95/46/CE. Aceeași concluzie se aplică setărilor browser-ului care ar permite în mod implicit vizarea utilizatorului (prin intermediul modulelor cookie). Acest aspect este explicat clar în noua formulare a articolului 5 alineatul (3), citat mai sus, în capitolul III.B.3. Aceste două exemple nu îndeplinesc în special cerințele pentru manifestarea neechivocă a voinței. Este esențial ca persoana vizată să aibă posibilitatea de a lua o decizie și de a o exprima, de exemplu prin bifarea efectivă a unei căsuțe, în vederea scopului prelucrării datelor.

În Avizul său privind publicitatea comportamentală, grupul de lucru a concluzionat că *„este esențial ca browserele să fie prevăzute cu setări prestabilite pentru protejarea confidențialității, cu alte cuvinte, să fie prevăzute cu setarea de <<neacceptare și netransmitere a modulelor cookie de la terți>>. Pentru a completa această setare și pentru a-i spori eficiența, browserele ar trebui să impună utilizatorilor să lanseze un asistent de protejare a confidențialității atunci când instalează pentru prima dată sau actualizează browserul și să prevadă o modalitate ușoara de exercitare a dreptului de alegere în timpul utilizării*[46]

III.B.5. <u>Articolul 6 alineatul (3), articolul (9) alineatele (3) și (4) – posibilitatea de a-și retrage consimțământul</u>

„ ... posibilitatea de a-și retrage acordul în orice moment ..."

Posibilitatea de a-și retrage consimțământul, care este implicită în Directiva 95/46/CE, este preluată în diferite dispoziții ale Directivei asupra confidențialității și comunicațiilor electronice. Acest aspect a fost menționat explicit în Avizul grupului de lucru privind utilizarea datelor de localizare în vederea furnizării de servicii cu valoare adăugată[47]:

„*În temeiul articolului 9 din Directiva 2002/58/CE, persoanele care și-au dat consimțământul pentru prelucrarea datelor de localizare, altele decât datele de*

[45] Avizul 5/2004 privind comunicațiile nesolicitate în scopuri de marketing în temeiul articolului 13 din Directiva 2002/58/CE, adoptat la 27.2.2004.

[46] Avizul din 22.6. 2010, WP 171, op.cit.

[47] Avizul 5/2005 privind utilizarea datelor de localizare în vederea furnizării de servicii cu valoare adăugată, adoptat la 25.11.2005 (WP115).

transfer, pot să-şi retragă consimţământul în orice moment şi trebuie să aibă posibilitatea, prin mijloace simple şi în mod gratuit, să refuze temporar prelucrarea acestor date. Grupul de lucru consideră aceste drepturi – care pot fi interpretate în sensul aplicării dreptului de a se opune la prelucrarea datelor de localizare – ca fiind esenţiale, având în vedere caracterul sensibil al datelor de localizare. Grupul de lucru consideră că informarea persoanelor, nu numai atunci când se abonează la un serviciu, ci şi atunci când îl utilizează, reprezintă o condiţie prealabilă pentru exercitarea acestor drepturi. În cazul în care, pentru furnizarea unui serviciu, este necesară prelucrarea continuă a datelor de localizare, Grupul de lucru este de părere că furnizorul serviciului ar trebui să reamintească periodic persoanei vizate că echipamentul său terminal a fost, va fi sau poate fi localizat. Aceasta permite persoanei respective să-şi exercite dreptul de a-şi retrage consimţământul, în temeiul articolului 9 din Directiva 2002/58/CE, în cazul în care doreşte acest lucru."

Astfel cum s-a menţionat anterior, aceasta implică faptul că retragerea are efect în viitor, nu pentru prelucrarea datelor desfăşurată în trecut, în perioada în care datele au fost colectate în mod legal. Deciziile sau acţiunile întreprinse anterior în temeiul acestor informaţii pot aşadar să nu fie pur şi simplu anulate. Cu toate acestea, dacă nu există un alt temei juridic care justifică continuarea stocării datelor, acestea ar trebui şterse de către operatorul de date.

IV. Concluzii

Prezentul aviz analizează cadrul juridic al utilizării consimţământului în temeiul Directivei 95/46/CE şi al Directivei 2002/58/CE. Scopul acestei acţiuni este dublu: în primul rând, se urmăreşte clarificarea cerinţelor legale existente şi ilustrarea modului în care acestea funcţionează în practică. În acelaşi timp, se analizează dacă mai este adecvat cadrul existent, având în vedere noile modalităţi multiple de prelucrare a datelor cu caracter personal sau dacă sunt necesare modificări.

IV.1. Clarificarea aspectelor cheie ale cadrului juridic actual

Articolul 2 litera (h) din Directiva 95/46/CE defineşte consimţământul ca „orice manifestare de voinţă liberă, specifică şi informată prin care persoana vizată acceptă să fie prelucrate datele cu caracter personal care o privesc". Articolul 7 din directivă, care oferă temeiul juridic pentru prelucrarea datelor cu caracter personal, desemnează consimţământul *neechivoc* ca unul dintre temeiurile juridice. Articolul 8 stabileşte consimţământul *explicit* ca temei juridic pentru prelucrarea datelor sensibile. Articolul 26 alineatul (1) din Directiva 95/46/CE şi diferite dispoziţii ale Directivei asupra confidenţialităţii şi comunicaţiilor electronice impun obţinerea consimţământului pentru anumite activităţi de prelucrare a datelor în sfera lor de aplicare. Aspectele abordate în prezentul aviz urmăresc să clarifice diferitele elemente ale acestui cadru juridic pentru ca acesta să fie mai uşor de aplicat în general de către părţile interesate.

Elemente/observaţii de natură generală

- Consimţământul este unul dintre cele şase temeiuri juridice pentru prelucrarea datelor cu caracter personal (unul dintre cele cinci temeiuri pentru datele sensibile); acesta este un temei juridic important deoarece permite persoanei vizate să aibă un anumit control asupra prelucrării datelor sale. Relevanţa consimţământului ca factor

care facilitează autonomia și autodeterminarea persoanei se bazează pe utilizarea sa în contextul adecvat și împreună cu elementele necesare.

- În general, cadrul juridic al Directivei 95/46/CE se aplică în orice situație în care se solicită consimțământul, în context offline sau online. De exemplu, aceleași reguli se aplică dacă un distribuitor de cărămizi și mortar propune clienților înregistrarea pentru un sistem de carduri de loialitate printr-un formular pe suport hârtie sau dacă acesta propune completarea formularului pe site-ul său internet. În plus, Directiva asupra confidențialității și comunicațiilor electronice menționează anumite operațiuni de prelucrare a datelor care fac obiectul consimțământului: acestea se referă în principal la prelucrarea datelor în legătură cu furnizarea de servicii publice de comunicații electronice. Condițiile pentru ca acordarea consimțământului să fie valabilă, prevăzute în Directiva 2002/58/CE, sunt aceleași cu cele prevăzute în Directiva 95/46/CE.

- Situațiile în care operatorii de date utilizează consimțământul ca temei juridic pentru prelucrarea datelor cu caracter personal nu trebuie confundate cu situațiile în care operatorul își fondează prelucrarea pe alte temeiuri juridice care implică dreptul individual de opoziție. De exemplu, atunci când prelucrarea este justificată de „interesele legitime" ale operatorului de date, conform articolului 7 litera (f) din Directiva 95/46/CE, persoana vizată are dreptul să se opună conform articolului 14 litera (a) din Directiva 95/46/EC. Un alt exemplu este situația în care operatorul de date trimite clienților săi curenți comunicații prin e-mail pentru a-și promova propriile produse și servicii sau produse și servicii similare; totuși, clienții au dreptul să se opună, conform articolului 13 alineatul (2) din Directiva 2002/58/CE. În ambele cazuri, persoana vizată are dreptul să se opună prelucrării, ceea ce este diferit față de consimțământ.

- Utilizarea consimțământului ca temei juridic pentru prelucrarea datelor cu caracter personal nu scutește operatorul de date de obligația de a respecta celelalte cerințe ale cadrului juridic privind protecția datelor, de exemplu, respectarea principiului proporționalității în conformitate cu articolul 6 alineatul (1) litera (c), al securității prelucrării conform articolului 17 etc.

- Consimțământul valabil presupune ca persoana vizată să aibă capacitatea juridică de a-și da consimțământul. Normele referitoare la capacitatea juridică pentru exprimarea consimțământului nu sunt armonizate și, prin urmare, pot varia de la un stat membru la altul.

- Persoanele care și-au acordat consimțământul trebuie să aibă posibilitatea de a și-l retrage, împiedicând astfel continuarea prelucrării datelor lor. Această dispoziție figurează și în Directiva asupra confidențialității și comunicațiilor electronice cu privire la anumite operațiuni de prelucrare a datelor care necesită acordarea consimțământului, precum prelucrarea datelor de localizare, altele decât datele de transfer.

- Consimțământul trebuie să fie acordat înainte de începerea prelucrării datelor cu caracter personal, însă acesta poate fi solicitat și în cursul prelucrării, în cazul în care există un nou scop de prelucrare. Acest aspect este subliniat în diferite dispoziții ale Directivei 2002/58/CE fie prin menționarea termenului „prealabil" [de exemplu, articolul 6 alineatul (3)], fie prin formularea dispoziției [de exemplu, articolul 5 alineatul (3)].

Elemente specifice ale cadrului juridic privind consimțământul

- Pentru a fi valabil, consimțământul trebuie să fie *liber exprimat*. Aceasta înseamnă că nu trebuie să existe niciun risc de înșelăciune, intimidare sau consecințe negative semnificative pentru persoana vizată dacă aceasta nu consimte la prelucrarea datelor. Operațiunile de prelucrare a datelor în contextul ocupării forței de muncă, unde intervine aspectul ierarhic, precum și în contextul serviciilor de stat, cum ar fi sănătatea, necesită o analiză atentă pentru a stabili dacă persoanele vizate sunt libere să-și exprime consimțământul.

- Consimțământul trebuie să fie *specific*. Consimțământul superficial, fără a preciza scopul exact, nu îndeplinește această condiție. Este mai bine ca, în cazul contractelor, să se utilizeze clauze specifice de consimțământ, separate de termenii și condițiile generale, decât să se includă această informație în cadrul condițiilor generale ale contractului.

- Consimțământul trebuie să fie *informat*. Articolele 10 și 11 din directivă enumeră tipurile de informații care trebuie să fie neapărat oferite persoanelor vizate. În orice caz, informațiile oferite trebuie să fie suficiente pentru a garanta că persoanele pot lua decizii în deplină cunoștință de cauză cu privire la prelucrarea datelor cu caracter personal care îi privesc. Necesitatea caracterului „informat" al consimțământului determină două cerințe suplimentare. În primul rând, modalitatea în care sunt oferite informațiile trebuie să ofere garanții, prin utilizarea unui limbaj adecvat, că persoanele vizate înțeleg pentru ce își acordă consimțământul și în ce scop. Această cerință este contextuală. Utilizarea unui limbaj juridic sau tehnic excesiv de complicat nu respectă cerințele legii. În al doilea rând, informațiile furnizate utilizatorilor trebuie să fie clare și suficient de evidente încât utilizatorii să le observe cu ușurință și să nu le poată trece cu vederea. Informațiile trebuie furnizate direct persoanelor vizate. Nu este suficient ca acestea să fie disponibile undeva.

- În ceea ce privește modul în care trebuie să se acorde consimțământul, articolul 8 alineatul (2) litera (a) impune acordarea consimțământului *explicit* pentru prelucrarea datelor sensibile, ceea ce presupune un răspuns activ, verbal sau în scris, prin care persoana vizată își exprimă dorința ca datele sale să fie prelucrate pentru anumite scopuri. Așadar, consimțământul expres nu poate fi obținut prin introducerea unei căsuțe bifate în prealabil. Persoana vizată trebuie să întreprindă o acțiune clară pentru a-și arăta consimțământul și trebuie să aibă posibilitatea de a nu consimți.

- Pentru alte categorii de date decât cele sensibile, articolul 7 alineatul (a) stipulează că acordarea consimțământului trebuie să se facă în mod *neechivoc*. Acest termen presupune utilizarea unor mecanisme de obținere a consimțământului care nu lasă loc de îndoieli cu privire la intenția persoanei vizate de a-și da consimțământul. În practică, această cerință permite operatorilor de date să utilizeze diferite tipuri de mecanisme de obținere a consimțământului, de la declarații de exprimare a acordului (consimțământ expres) până la mecanisme bazate pe acțiuni care arată acordul.

- Consimțământul bazat pe inacțiunea sau tăcerea persoanei vizate nu constituie în mod normal un consimțământ valid, în special în context online. Acesta este un aspect legat în special de utilizarea setărilor prestabilite, pe care persoana vizată este nevoită să le modifice pentru a refuza prelucrarea. Se poate da ca exemplu

utilizarea căsuțelor deja bifate sau a setărilor browser-ului de internet, care sunt prestabilite să colecteze date.

IV.2 Evaluarea cadrului juridic actual și necesitatea potențială de a aduce modificări

Evaluare generală

Grupul de lucru consideră că, în prezent, cadrul juridic privind protecția datelor conține o serie de norme bine concepute care stabilesc condițiile de valabilitate a consimțământului în vederea asigurării legalității operațiunilor de prelucrare a datelor. Acestea se aplică atât în context offline, cât și online. Mai precis:

Cadrul juridic reușește să stabilească un echilibru între o serie de preocupări. Pe de o parte, acesta asigură că numai consimțământul autentic, informat este considerat ca atare. În această privință, cerința explicită de la articolul 2 litera (h) conform căreia consimțământul trebuie să fie liber, specific și informat, este relevantă și satisfăcătoare. Pe de altă parte, această cerință nu este rigidă, ci oferă suficientă flexibilitate, evitând normele specifice de natură tehnică. Acest fapt este ilustrat tot de articolul 2 litera (h), în care consimțământul este definit ca fiind orice manifestare de voință a persoanei vizate. Această formulare oferă suficientă libertate în ceea ce privește modul în care manifestarea poate fi realizată. Articolele 7 și 8, care impun consimțământul neechivoc și, respectiv, explicit, surprind în mod adecvat echilibrul necesar dintre cele două preocupări, oferind flexibilitate, evitând structurile excesiv de rigide și garantând, în același timp, o protecție adecvată.

Rezultă, prin urmare, un cadru juridic care, dacă este aplicat și implementat în mod corespunzător, este capabil să se adapteze gamei largi de operații de prelucrare a datelor care decurg adesea din evoluția tehnologică.

Totuși, în practică, stabilirea cazurilor în care este necesar consimțământul și, în special, a cerințelor pentru consimțământul valabil, inclusiv modalitatea în care acestea trebuie aplicate în mod concret, nu este întotdeauna simplă, din cauza lipsei de uniformitate la nivelul statelor membre. Punerea în aplicare a legislației UE la nivel național a condus la abordări diferite. Au fost identificate probleme specifice în timpul discuțiilor din cadrul grupului de lucru „articolul 29” care au condus la elaborarea prezentului aviz, probleme descrise în continuare.

Modificări posibile

- Conceptul de consimțământ neechivoc este util pentru crearea unui sistem care nu este excesiv de rigid, însă oferă un nivel înalt de protecție. Deși are potențialul de a crea un sistem rezonabil, din păcate, sensul său este adesea înțeles greșit sau pur și simplu ignorat. Cu toate că indicațiile și exemplele oferite anterior ar trebui să contribuie la sporirea securității juridice și la protecția drepturilor persoanelor vizate atunci când consimțământul este utilizat ca temei juridic, această situație pare să indice că sunt necesare modificări.
- Mai precis, grupul de lucru „articolul 29” consideră că termenul în sine („neechivoc”) ar trebui să fie mai bine clarificat în cadrul revizuirii cadrului juridic general privind protecția datelor. Clarificarea trebuie să se facă în sensul sublinierii faptului că acordarea consimțământului neechivoc necesită utilizarea unor

mecanisme care nu lasă loc de îndoieli cu privire la intenția persoanei vizate de a-și acorda consimțământul. În același timp, trebuie să se specifice faptul că utilizarea opțiunilor prestabilite pe care persoana vizată trebuie să le modifice pentru a refuza prelucrarea (consimțământul bazat pe tăcere) nu constituie ca atare consimțământ neechivoc. Acest lucru este în special valabil în context online.

- Pe lângă clarificarea descrisă anterior, grupul de lucru „articolul 29" face următoarele recomandări:

    i. *În primul rând,* să se introducă în definiția consimțământului de la articolul 2 litera (h) termenul „neechivoc" (sau un termen echivalent) pentru a întări ideea că numai consimțământul bazat pe declarații sau acțiuni care arată acordul constituie consimțământ valabil. Pe lângă faptul că sporește claritatea, această măsură aliniază conceptul de consimțământ de la articolul 2 litera (h) cu cerințele privind consimțământul valabil de la articolul 7. În plus, sensul termenului „neechivoc" ar putea fi mai bine explicat într-un considerent din viitorul cadru juridic.

    ii. *În al doilea rând,* în contextul obligației generale de asumare a răspunderii, operatorii de date ar trebui să fie în măsură să demonstreze obținerea consimțământului. Într-adevăr, dacă se pune un accent mai mare pe sarcina probei și operatorii de date trebuie să demonstreze că au obținut efectiv consimțământul persoanei vizate, aceștia se vor vedea obligați să instituie practici și mecanisme standard pentru solicitarea și dovedirea consimțământului neechivoc. Tipul de mecanism va depinde de context și ar trebui să țină seama de faptele și circumstanțele prelucrării, în special de riscurile acesteia.

- Grupul de lucru „articolul 29" nu este convins că dispozițiile legale ar trebui să includă consimțământul explicit ca regulă generală pentru toate tipurile de operații de prelucrare, inclusiv cele care se încadrează în prezent în domeniul de aplicare a articolului 7 din directivă. Acesta consideră că noțiunea de consimțământ neechivoc, care cuprinde consimțământul explicit, dar și consimțământul rezultat din *acțiuni* neechivoce ar trebui să rămână cerința standard. Această opțiune oferă mai multă flexibilitate operatorilor de date în obținerea consimțământului, iar procedura generală poate fi mai rapidă și mai ușor de aplicat.

- Au fost identificate mai multe aspecte ale cadrului juridic care se referă la consimțământ din modul de formulare, istoricul juridic, jurisprudența și avizele elaborate de grupul de lucru „articolul 29". Introducerea în mod expres a acestor aspecte în noul cadru legislativ privind protecția datelor ar aduce o mai mare securitate juridică. Se poate ține seama de următoarele elemente:

    i. Includerea unei clauze specifice care să prevadă dreptul persoanelor de a-și retrage consimțământul.

    ii. Consolidarea cerinței conform căreia consimțământul trebuie să fie acordat înainte de începerea prelucrării sau înainte de utilizarea ulterioară a datelor în scopuri care nu au fost prevăzute în consimțământul inițial, în cazul în care nu există un alt temei juridic care justifică prelucrarea.

iii. Includerea unor cerințe explicite privind calitatea (obligația de a furniza informații privind prelucrarea datelor astfel încât să fie înțelese cu ușurință, într-un limbaj clar și simplu) și accesibilitatea informațiilor (obligația ca informațiile să fie evidente, ușor de observat și direct accesibile). Acest aspect este esențial pentru ca persoanele vizate să poată lua decizii informate.

- În final, în ceea ce privește persoanele aflate în incapacitate juridică, ar putea fi introduse dispoziții care să asigure un grad de protecție mai înalt, inclusiv:

i. Clarificări privind circumstanțele în care consimțământul trebuie să fie obținut de la părinți sau de la reprezentantul unei persoane aflate în incapacitate, inclusiv limita de vârstă sub care acest tip de consimțământ este obligatoriu.

ii. Stabilirea obligației de a utiliza mecanisme de verificare a vârstei, care pot varia în funcție de circumstanțe, cum ar fi vârsta copiilor, tipul de prelucrare, gradul de risc al prelucrării și dacă informațiile sunt păstrate de operatorul de date sau puse la dispoziția terților;

iii. Cerința de a adapta informațiile adresate copiilor astfel încât aceștia să înțeleagă mai ușor ce înseamnă să li se colecteze datele și să-și exprime consimțământul în cunoștință de cauză;

iv. Garanții specifice de identificare a activităților de prelucrare a datelor, precum publicitatea comportamentală, în cadrul cărora consimțământul nu ar trebui să fie un temei pentru legitimizarea prelucrării datelor cu caracter personal.

Grupul de lucru „articolul 29" va mai aborda în viitor problema consimțământului. Mai precis, autoritățile naționale pentru protecția datelor, precum și grupul de lucru pot decide ulterior să elaboreze orientări pentru dezvoltarea prezentului aviz, oferind exemple practice suplimentare referitoare la utilizarea consimțământului.

Adoptat la Bruxelles, 13 iulie 2011

Pentru grupul de lucru,

Președintele
Jacob KOHNSTAMM